NETGEAR 7000 Series Managed Switch Administration Guide Version 7.2

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10238-02
May 2008

© 2008 by NETGEAR, Inc. All rights reserved.

Trademarks

NETGEAR and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc..

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders. Portions of this document are copyright Intoto, Inc.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Netgear's 7000 Series Managed Switch is compliant with the following EU Council Directives: 89/336/EEC and LVD 73/23/EEC. Compliance is verified by testing to the following standards: EN55022 Class A, EN55024 and EN60950-1.

Certificate of the Manufacturer/Importer

It is hereby certified that the 7000 Series Managed Switch has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

The Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das7000 Series Managed Switch gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class A category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas. When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

FCC Information to User

Declaration Of Conformity

We NETGEAR, Inc., 4500 Great America Parkway, Santa Clara, CA 95054, declare under our sole responsibility that the model 7000 Series Managed Switch complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

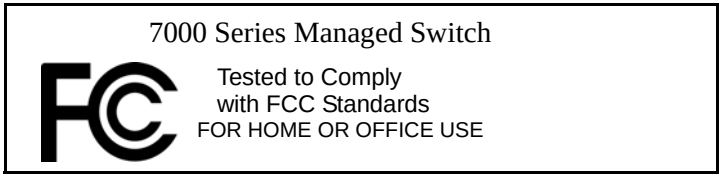
- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Requirements for Operation in the United States

Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the receiver
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected
- Consult the dealer or an experienced radio/TV technician for help.



Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (7000 Series Managed Switch) does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Product and Publication Details

Model Number:	7xxx
Publication Date:	May 2008
Product Family:	Managed Switch
Product Name:	7000 Series Managed Switch
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10238-02
Publication Version Number:	1.0

Contents

NETGEAR 7000 Series Managed Switch Administration Guide Version 7.2

About This Manual

Conventions, Formats and Scope xv
How to Use This Manual xvi
How to Print this Manual xvi
Revision History xvii

Chapter 1
Introduction

Document Organization 1-1
Audience 1-2
CLI Documentation 1-3
Related Documentation 1-3

Chapter 2
Getting Started

In-band and Out-of-band Connectivity 2-5
Configuring for In-band Connectivity 2-5
Using BootP or DHCP 2-5
Using the EIA-232 Port 2-6
Configuring for Out-Of-Band Connectivity 2-7
Starting the Switch 2-8
Initial Configuration 2-8
Initial Configuration Procedure 2-9
Software Installation 2-10
Quick Starting the Networking Device 2-10
System Information and System Setup 2-10

Chapter 3
Using Ezconfig for Switch Setup

Changing the Password 3-2

Setting Up the Switch IP Address 3-2
Assigning Switch Name and Location Information 3-3
Saving the Configuration 3-3

Chapter 4
Using the Web Interface

Configuring for Web Access 4-1
Starting the Web Interface 4-2
Web Interface Layout 4-2
Configuring an SNMP V3 User Profile 4-6

Chapter 5
Virtual LANs

VLAN Configuration Example 5-2
CLI Examples 5-2
Example #1: Create Two VLANs 5-2
Example #2: Assign Ports to VLAN2 5-3
Example #3: Assign Ports to VLAN3 5-3
Example #4: Assign VLAN3 as the Default VLAN 5-3
Graphical User Interface 5-4

Chapter 6 Link Aggregation

CLI Example 6-1
Example #1: Create two LAGS 6-2
Example #2: Add the ports to the LAGs 6-3
Example #3: Enable both LAGs 6-3

Chapter 7
IP Routing Services

Port Routing 7-1
Port Routing Configuration 7-2
CLI Examples 7-3
Example #1: Enabling routing for the Switch 7-3
Example #2: Enabling Routing for Ports on the Switch 7-4
VLAN Routing 7-4
VLAN Routing Configuration 7-5
CLI Examples 7-5
Example #1: Create Two VLANs 7-6
Example #2: Set Up VLAN Routing for the VLANs and the Switch. 7-6

VLAN Routing RIP Configuration 7-7
CLI Example 7-8
VLAN Routing OSPF Configuration 7-10
CLI Example 7-10
Routing Information Protocol 7-12
RIP Configuration 7-12
CLI Examples 7-13
Example #1: Enable Routing for the Switch 7-13
Example #2: Enable Routing for Ports 7-14
Example #3: Enable RIP for the Switch 7-14
Example #4: Enable RIP for ports 1/0/2 and 1/0/3 7-15
OSPF 7-15
CLI Examples 7-16
Example #1: Configuring an Inter-Area Router 7-17
Example #2: Configuring OSPF on a Border Router 7-19

Proxy Address Resolution Protocol (ARP) 7-21
Overview 7-21
CLI Examples 7-22
Example #1: show ip interface 7-22
Example #2: ip proxy-arp 7-22

Chapter 8
Virtual Router Redundancy Protocol

CLI Examples 8-2
Example #1: Configure VRRP on a Master Router 8-3
Example #2: Configure VRRP on a Backup Router 8-4

Chapter 9
Access Control Lists (ACLs)

Overview 9-1
Limitations 9-1
MAC ACLs 9-1
Configuring IP ACLs 9-2
Process 9-3
IP ACL Examples 9-3
Example #1: Set up an IP ACL with Two Rules 9-3

Example #2: Configure a One-Way Access Using a TCP Flag in an ACL 9-4
CLI Commands 9-5
Web Interface Procedure 9-8
Example #3: Configure Isolated VLANs on a Layer 3 switch by Using ACLs 9-23
CLI Commands 9-24
Web Interface Procedure 9-26
MAC ACL CLI Examples 9-38
Example #1: mac access list 9-38
Example #2: permit any 9-39
Example #3 Configure mac access-group 9-40
Example #4 permit 9-41
Example #5: show mac access-lists 9-42

Chapter 10
Class of Service (CoS) Queuing

Overview 10-1
CoS Queue Mapping 10-1
Trusted Ports 10-1
Untrusted Ports 10-2
CoS Queue Configuration 10-2
Port Egress Queue Configuration 10-2
Drop Precedence Configuration (per Queue) 10-3
Per-Interface Basis 10-3
CLI Examples 10-3
Example #1: show classofservice trust 10-4
Example #2: set classofservice trust mode 10-4
Example #3: show classofservice ip-precedence mapping 10-5
Example #4: Config Cos-queue Min-bandwidth and Strict Priority Scheduler Mode 10-5
Example #5: Set CoS Trust Mode of an Interface 10-6
Traffic Shaping 10-6
CLI Example 10-6
Example #1 traffic-shape 10-7

Chapter 11
Differentiated Services

CLI Example 11-2
DiffServ for VoIP Configuration Example 11-4

Chapter 12
IGMP Snooping

Overview 12-1
CLI Examples 12-1
Example #1: Enable IGMP Snooping 12-1
Example #2: show igmpsnooping 12-2
Example #3: show mac-address-table igmpsnooping 12-2

Chapter 13
Port Security

Overview 13-1
Operation 13-2
CLI Examples 13-3
Example #1: show port security 13-3
Example #2: show port security on a specific interface 13-3
Example #3: (Config) port security 13-3

Chapter 14
Traceroute

CLI Example 14-2

Chapter 15
Configuration Scripting

Overview 15-1
Considerations 15-1
CLI Examples 15-1
Example #1: script 15-2
Example #2: script list and script delete 15-2
Example #3: script apply running-config.scr 15-2
Example #4: Creating a Configuration Script 15-3
Example #5: Upload a Configuration Script 15-3

Chapter 16
Outbound Telnet

Overview 16-1
CLI Examples 16-1
Example #1: show network 16-2
Example #2: show telnet 16-2
Example #3: transport output telnet 16-3

Example #4: session-limit and session-timeout 16-3

Chapter 17 Port Mirroring

Overview 17-1
CLI Examples 17-1
Example #1: show monitor session 17-2
Example #2: show port all 17-2
Example #3: show port interface 17-2
Example #4: (Config) monitor session 1 mode 17-3
Example #5: (Config) monitor session 1 source interface 17-4
Example #6: (Interface) port security 17-4

Chapter 18
Simple Network Time Protocol (SNTP)

Overview 18-1
CLI Examples 18-1
Example #1: show sntp 18-1
Example #2: show sntp client 18-2
Example #3: show sntp server 18-2
Example #4: Configure SNTP 18-2
Example #5: Setting Time Zone 18-4
Example #6: Setting Named SNTP Server 18-4

Chapter 19
Syslog

Overview 19-1
Persistent Log Files 19-1
Interpreting Log Files 19-2
CLI Examples 19-2
Example #1: show logging 19-3
Example #2: show logging buffered 19-3
Example #3: show logging traplogs 19-4
Example #4: show logging hosts 19-4
Example #5: logging port configuration 19-5

Chapter 20
Managing Switch Stacks

Understanding Switch Stacks 20-2
Switch Stack Membership 20-3

Switch Stack Cabling (FSM73xxS) 20-4
Stack Master Election and Re-Election 20-5
Stack Member Numbers 20-5
Stack Member Priority Values 20-6
Switch Stack Offline Configuration 20-6
Effects of Adding a Preconfigured Switch to a Switched Stack 20-6
Effects of Replacing a Preconfigured Switch in a Switch Stack 20-7
Effects of Removing a Preconfigured Switch from a Switch Stack 20-7
Switch Stack Software Compatibility Recommendations 20-8
Incompatible Software and Stack Member Image Upgrades 20-8
Switch Stack Configuration Files 20-8
Switch Stack Management Connectivity 20-9
Connectivity to the Switch Stack Through Console Ports 20-9
Connectivity to the Switch Stack Through Telnet 20-9
Switch Stack Configuration Scenarios 20-9
Stacking Recommendations 20-11
General Practices 20-11
Initial installation and Power-up of a Stack 20-12
Removing a Unit from the Stack 20-12
Adding a Unit to an Operating Stack 20-13
Replacing a Stack Member with a New Unit 20-13
Renumbering Stack Members 20-14
Moving a Master to a Different Unit in the Stack 20-14
Removing a Master Unit from an Operating Stack 20-14
Merging Two Operational Stacks 20-15
Preconfiguration 20-15
Upgrading Firmware 20-15
Migration of Configuration With a Firmware Upgrade 20-16
Code Mismatch 20-17

Chapter 21
Pre-Login Banner

Overview 21-1
CLI Example 21-1
Example 1#: Create a Pre-Login Banner 21-1

Chapter 22
IGMP Querier

CLI Examples 22-2
Example #1: Enable IGMP Querier 22-2
Example #2: Show IGMP Querier Status 22-2

Chapter 23
DNS

Overview 23-1
Examples 23-1
Example 1#: Specify Two DNS Servers 23-1
CLI Commands 23-2
Web Interface Procedure 23-2
Example 2#: Manually Add a Host Name and an IP Address 23-3
CLI Commands 23-3
Web Interface Procedure 23-3

Chapter 24
DHCP Server

Overview 24-1
Examples 24-1
Example 1#: Configure DHCP Server in Dynamic Mode 24-1
CLI Commands 24-1
Web Interface Procedure 24-2
Example #2: Configure a DHCP Server in Manual Mode 24-4
CLI Commands 24-4
Web Interface Procedure 24-5

Chapter 25
Protected Ports

Overview 25-1
Example 25-1
Example #1: Configure a Protected Port to Isolate Ports on the Switch 25-1
CLI Commands 25-2
Web Interface Procedure 25-3

Chapter 26
802.1x Port Security

Overview 26-1

Example 26-1
Example 1#: Enable 802.1x Authentication on One Port in a VLAN 26-1
CLI Commands 26-2
Web Interface Procedure 26-3
Chapter 27
Double VLANs
Overview 27-1
Example 27-1
Example 1#: Enable a Double VLAN on a VLAN 27-1
CLI Commands 27-2
Web Interface Procedure 27-3
Index

About This Manual

The *NETGEAR 7000 Series Managed Switch Administration Guide Version 7.2* describes how to install, configure and troubleshoot the 7000 Series Managed Switch. The information in this manual is intended for readers with intermediate computer and Internet skills.

Conventions, Formats and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical Conventions.** This manual uses the following typographical conventions:

Italics	Emphasis, books, CDs, URL names
Bold	User input
`Fixed`	Screen text, file and server names, extensions, commands, IP addresses

- **Formats.** This manual uses the following formats to highlight special messages:

	Note: This format is used to highlight information of importance or special interest.

	Tip: This format is used to highlight a procedure that will save time or resources.

	Warning: Ignoring this type of note may result in a malfunction or damage to the equipment.

	Danger: This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

- **Scope.** This manual is written for the 7000 Series Managed Switch according to these specifications:

Product Version	7000 Series Managed Switch
Manual Publication Date	May 2008

Note: Product updates are available on the NETGEAR, Inc. website at *http://kbserver.netgear.com/products/7xxx.asp*.

How to Use This Manual

The HTML version of this manual, if provided, includes the following:

- Buttons, > and <, for browsing forwards or backwards through the manual one page at a time
- A button that displays the table of contents and an button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

To print this manual, you can choose one of the following options, according to your needs.

- **Printing a Page from HTML**. Each page in the HTML version of the manual is dedicated to a major topic. Select File > Print from the browser menu to print the page contents.
- **Printing from PDF**. Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.
  - **Printing a PDF Chapter.** Use the *PDF of This Chapter* link at the top left of any page.

- Click the *PDF of This Chapter* link at the top left of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.
- Click the print icon in the upper left of your browser window.

– **Printing a PDF version of the Complete Manual**. Use the *Complete PDF Manual* link at the top left of any page.

- Click the *Complete PDF Manual* link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.
- Click the print icon in the upper left of your browser window.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Revision History

Part Number	Version Number	Description
202-10238-01	1.0	Product update: New firmware and new user Interface
202-10238-02	1.0	The following changes were made: • The Web Interface Layout section in Chapter 4, Using the Web Interface, was changed to introduce the Prosafe Control Center. • New CLI and Web interface examples were added to the IP ACL Examples section in Chapter 9, Access Control Lists (ACLs). • Chapter 23, DNS, was added. • Chapter 24, DHCP Server, was added. • Chapter 25, Protected Ports, was added. • Chapter 26, 802.1x Port Security, was added. • Chapter 27, Double VLANs, was added.

Chapter 1
Introduction

This document provides an understanding of the CLI and Web configuration options for software Release 7.2 features.

Document Organization

This document provides examples of the use of the switch software in a typical network. It describes the use and advantages of specific functions provided by the 7000 Series Managed Switch, and includes information on configuring those functions using the Command Line Interface and Web Interface.

The switch software can operate as a Layer 2 switch, a Layer 3 router, or a combination switch/router. The switch also includes support for network management and Quality of Service functions such as Access Control Lists and Differentiated Services. Which functions you choose to activate will depend on the size and complexity of your network: this document describes configuration for some of the most-used functions.

This document contains configuration information about the following:

- Layer 2
  - VLANs
- Layer 3
  - Port routing
  - VLAN Routing
  - Virtual Router Redundancy Protocol (VRRP)
  - RIP
  - OSPF
  - Proxy ARP
- Quality of Service (QoS)
  - Access Control Lists (ACLs)

  - Class of Service (CoS)
  - Differentiated Services
- Multicast
  - IGMP Snooping
- Security
  - Denial of Service
  - Port Security
- Operating System
  - Dual Configuration
- Tools
  - Alarm Manager
  - Traceroute
  - Configuration Scripting
  - Advance Keying
  - Prelogin Banner
  - Port Mirroring
  - SNTP
  - Syslog
  - Data Migration

Audience

Use this guide if you are a(n):

- Experienced system administrator who is responsible for configuring and operating a network using switch software
- Level 1 and Level 2 Support provider

To obtain the greatest benefit from this guide, you should have an understanding of the switch software base and should have read the specification for your networking device platform. You should also have a basic knowledge of Ethernet and networking concepts.

CLI Documentation

The *Command Line Reference* provides information about the CLI commands used to configure the switch and the stack. The document provides CLI descriptions, syntax, and default values.

Refer to the *Command Line Reference* for information for the command structure

Related Documentation

Before proceeding, read the Release Notes for this switch product. The Release Notes detail the platform specific functionality of the Switching, Routing, SNMP, Config, Management, and other packages. In addition, see the following publications:

- Netgear Quick Installation Guide, 7000 Series Managed Switch
- Netgear CLI Reference for the Prosafe 7X00 Series Managed Switch. There are three documents in this series; choose the appropriate one for your product.
- Netgear Hardware Installation Guide for your switch

These documents may be found at *http://www.NETGEAR.com*.

Chapter 2
Getting Started

Connect a terminal to the switch to begin configuration.

In-band and Out-of-band Connectivity

Ask the system administrator to determine whether you will configure the switch for in-band or out-of-band connectivity.

Configuring for In-band Connectivity

In-band connectivity allows you to access the switch from a remote workstation using the Ethernet network. To use in-band connectivity, you must configure the switch with IP information (IP address, subnet mask, and default gateway).

Configure for In-band connectivity using one of the following methods:

- BootP or DHCP
- EIA-232 port

Using BootP or DHCP

You can assign IP information initially over the network or over the Ethernet service port through BootP or DHCP. Check with your system administrator to determine whether BootP or DHCP is enabled.

You need to configure the BootP or DHCP server with information about the switch—obtain this information through the serial port connection using the **show network** command. Set up the server with the following values:

IP Address	Unique IP address for the switch. Each IP parameter is made up of four decimal numbers, ranging from 0 to 255. If there is no DHCP server available to assign an IP address to the switch via DHCP, the default IP address for the switch is 169.254.100.100.
Subnet	Subnet mask for the LAN

gateway	IP address of the default router, if the switch is a node outside the IP range of the LAN
MAC Address	MAC address of the switch

When you connect the switch to the network for the first time after setting up the BootP or DHCP server, it is configured with the information supplied above. The switch is ready for in-band connectivity over the network.

If you do not use BootP or DHCP, access the switch through the EIA-232 port, and configure the network information as described below.

Using the EIA-232 Port

You can use a locally or remotely attached terminal to configure in-band management through the EIA-232 port.

1. To use a locally attached terminal, attach one end of a null-modem serial cable to the EIA-232 port of the switch and the other end to the COM port of the terminal or workstation.
   For remote attachment, attach one end of the serial cable to the EIA-232 port of the switch and the other end to the modem.
2. Set up the terminal for VT100 terminal emulation.
   a. Set the terminal ON.
   b. Launch the VT100 application.
3. Configure the COM port as follows:
   a. Set the data rate to 9600 baud.
   b. Set the data format to 8 data bits, 1 stop bit, and no parity.
   c. Set the flow control to none.
   d. Select the proper mode under **Properties**.
   e. Select Terminal keys.

The Log-in User prompt displays when the terminal interface initializes.

4. Enter an approved user name and password. The default is *admin* for the user name and the *password* is blank.
   The switch is installed and loaded with the default configuration.
5. Reduce network traffic by turning off the Network Configuration Protocol. Enter the following command:

```
configure network protocol none
```

6. Set the IP address, subnet mask, and gateway address by issue the following command:
`config network parms` *`ipaddress netmask gateway`*

IP Address	Unique IP address for the switch. Each IP parameter is made up of four decimal numbers, ranging from 0 to 255. The default IP address is 169.254.100.100.
Subnet	Subnet mask for the LAN. The default value is 255.255.255.0.
gateway	IP address of the default router, if the switch is a node outside the IP range of the LAN.

7. To enable these changes to be retained during a reset of the switch, type **Ctrl-Z** to return to the main prompt, type **save config** at the main menu prompt, and type **y** to confirm the changes.

8. To view the changes and verify in-band information, issue the command: **show network**.

9. The switch is configured for in-band connectivity and ready for Web-based management.

Configuring for Out-Of-Band Connectivity

To monitor and configure the switch using out-of-band connectivity, use the console port to connect the switch to a terminal desktop system running terminal emulation software. The console port connector is a male DB-9 connector, implemented as a data terminal equipment (DTE) connector.

The following hardware is required to use the console port:

- VT100-compatible terminal, or a desktop, or a portable system with a serial port running VT100 terminal emulation software.
- An RS-232 crossover cable with a female DB-9 connector for the console port and the appropriate connector for the terminal.

Perform the following tasks to connect a terminal to the switch console port using out-of-band connectivity:

1. Connect an RS-232 crossover cable to the terminal running VT100 terminal emulation software.

2. Configure the terminal emulation software as follows:

a. Select the appropriate serial port (serial port 1 or serial port 2) to connect to the console.

b. Set the data rate to 9600 baud.

c. Set the data format to 8 data bits, 1 stop bit, and no parity.

d. Set the flow control to none.

e. Select the proper mode under **Properties**.

f. Select Terminal keys.

	Note: When using HyperTerminal with Microsoft Windows 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. With Windows 2000 Service Pack 2, the arrow keys function properly in HyperTerminal's VT100 emulation. Go to *www.microsoft.com* for more information on Windows 2000 service packs.

3. Connect the female connector of the RS-232 crossover cable directly to the switch console port, and tighten the captive retaining screws.

Starting the Switch

1. Make sure that the switch console port is connected to a VT100 terminal or VT100 terminal emulator via the RS-232 crossover cable.

2. Locate an AC power receptacle.

3. Deactivate the AC power receptacle.

4. Connect the switch to the AC receptacle.

5. Activate the AC power receptacle.

When the power is turned on with the local terminal already connected, the switch goes through a power-on self-test (POST). POST runs every time the switch is initialized and checks hardware components to determine if the switch is fully operational before completely booting. If POST detects a critical problem, the startup procedure stops. If POST passes successfully, a valid executable image is loaded into RAM. POST messages are displayed on the terminal and indicate test success or failure. The boot process runs for approximately 60 seconds.

Initial Configuration

The initial simple configuration procedure is based on the following assumptions:

- The switch was not configured before and is in the same state as when you received it.
- The switch booted successfully.

- The console connection was established and the console prompt appears on the screen of a VT100 terminal or terminal equivalent.

The initial switch configuration is performed through the console port. After the initial configuration, you can manage the switch either from the already-connected console port or remotely through an interface defined during the initial configuration.

The switch is not configured with a default user name and password.

All of the settings below are necessary to allow the remote management of the switch through Telnet (Telnet client) or HTTP (Web browser).

Before setting up the initial configuration of the switch, obtain the following information from your network administrator:

- The IP address to be assigned to the management interface through which the switch is managed.
- The IP subnet mask for the network.
- The IP address of the default gateway.

Initial Configuration Procedure

You can perform the initial configuration using the Easy Setup Wizard or by using the Command Line Interface (CLI). The Setup Wizard automatically starts when the switch configuration file is empty. You can exit the wizard at any point by entering [ctrl+z]. For more information on CLI initial configuration, see the *User's Configuration Guide*. This guide shows how to use the Setup Wizard for initial switch configuration. The wizard sets up the following configuration on the switch:

- Establishes the initial privileged user account with a valid password. The wizard configures one privileged user account during the set up.
- Enables CLI login and HTTP access to use the local authentication setting only.
- Sets up the IP address for the management interface.
- Sets up the SNMP community string to be used by the SNMP manager at a given IP address. You may choose to skip this step if SNMP management is not used for this switch.
- Allows you to specify the management server IP or permit SNMP access from all IP addresses.
- Configures the default gateway IP address.

Software Installation

This section contains procedures to help you become acquainted quickly with the switch software.

Before installing switch software, you should verify that the switch operates with the most recent firmware.

Quick Starting the Networking Device

1. Configure the switch for In-band or Out-of-Band connectivity. In-band connectivity allows access to the software locally or from a remote workstation. You must configure the device with IP information (IP address, subnet mask, and default gateway).
2. Turn the Power ON.
3. Allow the device to load the software until the login prompt appears. The device initial state is called the default mode.
4. When the prompt asks for operator login, do the following steps:
   - Type `admin` at the login prompt. Since a number of the Quick Setup commands require administrator account rights, log in to an administrator account.
   - Do not enter a password because the default mode does not use a password.
   - Check the CLI User EXEC prompt is displayed.
   - Enter **`enable`** to switch to the Privileged EXEC mode from User EXEC.
   - Enter **`configure`** to switch to the Global Config mode from Privileged EXEC.
   - Enter **`exit`** to return to the previous mode.
   - Enter **`?`** to show a list of commands that are available in the current mode.

System Information and System Setup

This section describes the commands you use to view system information and to setup the network device. Table 2-1 contains the Quick Start commands that allow you to view or configure the following information:

- Software versions
- Physical port data
- User account management
- IP address configuration

- Uploading from Networking Device to Out-of-Band PC (Only XMODEM)
- Downloading from Out-of-Band PC to Networking Device (Only XMODEM)
- Downloading from TFTP Server
- Restoring factory defaults

If you configure any network parameters, you should execute the following command:

```
copy system:running-config nvram:startup-config
```

This command saves the changes to the configuration file. You must be in the correct mode to execute the command. If you do not save the configuration, all changes are lost when a you power down or reset the networking device. In a stacking environment, the running configuration is saved in all units of the stack.

Table 2-1 describes the command syntax, the mode you must be in to execute the command, and the purpose and output of the command.

Table 2-1. Quick Start Commands

Command	Mode	Description
show hardware	Privileged EXEC	Shows hardware version, MAC address, and software version information.
show users	Privileged EXEC	Displays all of the users that are allowed to access the networking device. Access Mode shows whether you can change parameters on the networking device (Read/Write) or can only view them (Read Only). As a factory default, the ‘admin’ user has Read/Write access and the ‘guest’ user has Read Only access. There can only be one Read/Write user. There can be up to five Read Only users.
show loginsession	User EXEC	Displays all of the login session information.
users passwd *<username>*	Global Config	Allows the user to set passwords or change passwords needed to login. A prompt appears after the command is entered requesting the users old password. In the absence of an old password leave the area blank. User password should not be more than eight characters in length.

Table 2-1. Quick Start Commands

Command	Mode	Description
copy system:running-config nvram:startup-config	Privileged EXEC	Saves passwords and all other changes to the device. If you do not save the configuration, all changes are lost when you power down or reset the networking device. In a stacking environment, the running configuration is saved in all units of the stack.
logout	User EXEC Privileged EXEC	Logs the user out of the networking device.
show network	User EXEC	Displays the following network configuration information: • IP Address - IP Address of the interface (default: 0.0.0.0) • Subnet Mask - IP Subnet Mask for the interface (default: 0.0.0.0) • Default Gateway - The default Gateway for this interface (default: 0.0.0.0) • Burned in MAC Address - The Burned in MAC Address used for in-band connectivity • Locally Administered MAC Address - Can be configured to allow a locally administered MAC address • MAC Address Type - Specifies which MAC address should be used for in-band connectivity • Network Configurations Protocol Current - Indicates which network protocol is being used (default: none) • Management VLAN Id - Specifies VLAN id • Web Mode - Indicates whether HTTP/Web is enabled. • Java Mode - Indicates whether java mode is enabled.
network parms *<ipaddr> <netmask> [gateway]*	Privileged EXEC	Sets the IP address, subnet mask and gateway of the router. The IP address and the gateway must be on the same subnet. IP address range is from 0.0.0.0 to 255.255.255.255.
copy nvram:startup-config *<tftp://<ipaddress>/<filepath>/<filename>>*	Privileged EXEC	Starts the configuration file upload, displays the mode and type of upload and confirms the upload is progressing. The URL must be specified as: xmodem:<filepath>/<filename> For example: If the user is using HyperTerminal, the user must specify where the file is going to be received by the PC.

Table 2-1. Quick Start Commands

Command	Mode	Description
copy nvram:error-log *<tftp://<ipaddress>/<filepath>/<filename>>*	Privileged EXEC	Starts the error log upload, displays the mode and type of upload and confirms the upload is progressing. The URL must be specified as: xmodem:<filepath>/<filename>
copy nvram:traplog *<tftp://<ipaddress>/<filepath>/<filename>>*	Privileged EXEC	Starts the trap log upload, displays the mode and type of upload and confirms the upload is progressing. The URL must be specified as: xmodem:<filepath>/<filename>
copy *<tftp://<ipaddress>/<filepath>/<filename>>* **nvram:startup-config**	Privileged EXEC	Sets the destination (download) datatype to be an image (system:image) or a configuration file (nvram:startup-config). The URL must be specified as: xmodem:<filepath>/<filename> For example: If the user is using Hyper Terminal, the user must specify which file is to be sent to the networking device. The Networking Device restarts automatically once the code has been downloaded.
copy *<tftp://<ipaddress>/<filepath>/<filename>>* **system:image**	Privileged EXEC	Sets the destination (download) datatype to be an image (system:image) or a configuration file (nvram:startup-config). The URL must be specified as: xmodem:<filepath>/<filename>
copy *<tftp://<ipaddress>/<filepath>/<filename>>* **nvram:startup-config**	Privileged EXEC	Sets the destination (download) datatype to be a configuration file. The URL must be specified as: tftp://<ipaddress>/<filepath>/<filename> Before starting a TFTP server download, you must configure the IP address.

Table 2-1. Quick Start Commands

Command	Mode	Description
copy *<tftp://<ipaddress>/<filepath>/<filename>>* **system:image**	Privileged EXEC	Sets the destination (download) datatype to be an image. The URL must be specified as: tftp://<ipaddress>/<filepath>/<filename> The system:image option downloads the code file.
clear config	Privileged EXEC	Enter yes when the prompt asks if you want to clear all the configurations made to the networking device.
copy system:running-config nvram:startup-config	Privileged EXEC	Enter yes when the prompt asks if you want to save the configurations made to the networking device.
reload (or cold boot the networking device)	Privileged EXEC	Enter yes when the prompt asks if you want to reset the system. You can reset the networking device or cold boot the networking device. Both work effectively.

Chapter 3
Using Ezconfig for Switch Setup

Ezconfig is an interactive utility that provides a simplified procedure for setting up the following switch parameters:

- Switch management IP address
- Switch admin user password
- Switch name and location

Ezconfig can be entered either in Global Config mode (#) or in Display mode (>).

The utility displays the following text when you enter the **`ezconfig`** command

```
(FSM7352S) >ezconfig

NETGEAR EZ Configuration Utility
--------------------------------
Hello and Welcome!
This utility will walk you through assigning the IP address for the switch
management CPU. It will allow you to save the changes at the end. After the
session, simply use the newly assigned IP address to access the Web GUI using
any public domain Web browser.

Admin password not defined. Do you want to change the password? (Y/N/Q)
```

Note: At any point in the setup, you can type **`Q`** to abort the program. At this point, *Ezconfig* will check if there is any change, and prompt you if the changes should be saved

Changing the Password

The first question it will ask is whether you wish to change the admin password. For security reasons, you should change the password by typing **Y**. If you have already set the password and do not wish to change it again, just enter **N**.

```
Enter new password:********
Confirm new password:********
Password Changed!

The 'enable' password required for switch configuration via the command line
interface is currently not configured. Do you wish to change it (Y/N/Q)?  y


Enter new password:********
Confirm new password:********
Password Changed!
```

Setting Up the Switch IP Address

After the password for both Admin and Enable mode is changed, you will be prompted to setup the IP address of the switch.

```
Assigning an IP address to your switch management

Current IP Address Configuration
--------------------------------
IP address: 0.0.0.0
Subnet mask: 0.0.0.0

Would you like to assign an IP address now (Y/N/Q)?  y

IP Address:
```

Ezconfig will display the current IP address and subnet mask. By default, the network management IP address uses DHCP protocol to have a DHCP server assign its IP address automatically. However, you can overwrite the DHCP client mode by assigning a fixed IP address here. Once a fixed IP address is assigned, *Ezconfig* automatically disables DHCP client mode and assigns the static IP address to the management VLAN.

If an IP address is already assigned, and you do not wish to change the IP address again, simply type **N.**

Assigning Switch Name and Location Information

Ezconfig will proceed to the next step in the setup:

```
Do you want to assign switch name and location information (Y/N/Q)?

System Name: Alpha1-1
System Location: Bld1
System Contact: James

There are changes detected, do you wish to save the changes permanently (Y/N)?
```

Note: The System Name, System Location and System Contact fields accept only alphanumeric characters, characters like "#$…" are not supported.

Note: The maximum length of the value cannot be longer than 31 bytes.

Saving the Configuration

After the name and location values are entered, *Ezconfig* will ask if you would like to have the changes be saved into the Flash (permanently storage). Enter **Y** to save the configuration.

```
There are changes detected, do you wish to save the changes permanently (Y/N)?
y

The configuration changes have been saved successfully.
Please enter 'show running-config' to see the final configuration.

Thanks for using EzConfig!
```

If during the session, the switch loses its power, the setup information will be lost if *Ezconfig* does not have the chance to save the changes before power-down.

Chapter 4
Using the Web Interface

This chapter is a brief introduction to the web interface; for example, it explains how to access the Web-based management panels to configure and manage the system.

Tip: Use the Web interface for configuration instead of the CLI interface. Web configuration is quicker and easier than entering the multiple required CLI commands. There are equivalent functions in the Web interface and the terminal interface—that is, both applications usually employ the same menus to accomplish a task. For example, when you log in, there is a Main Menu with the same functions available.

You can manage your switch through a Web browser and Internet connection. This is referred to as Web-based management. To use Web-based management, the system must be set up for in-band connectivity.

To access the switch, the Web browser must support:

- HTML version 4.0, or later
- HTTP version 1.1, or later
- JavaScript™ version 1.2, or later

There are several differences between the Web and terminal interfaces. For example, on the Web interface the entire forwarding database can be displayed, while the terminal interface only displays 10 entries starting at specified addresses.

To terminate the Web login session, close the web browser.

Configuring for Web Access

To enable Web access to the switch:

1. Configure the switch for in-band connectivity. The switch *Getting Started Guide* provides instructions.

2. Enable Web mode:
   a. At the CLI prompt, enter the **show network** command.
   b. Set **Web Mode** to Enabled.

Starting the Web Interface

Follow these steps to start the switch Web interface:

1. Enter the IP address of the switch in the Web browser address field.
2. When the Login panel is displayed click **Login**.
3. .Enter the appropriate User Name and Password. The User Name and associated Password are the same as those used for the terminal interface. Click on the Login button.
4. The System Description Menu displays, with the navigation tree appearing to the left of the screen.
5. Make a selection by clicking on the appropriate item in the navigation tree.

Web Interface Layout

As of software release 7.2, the Web interface has a new look. The new Web interface is called the Prosafe Control Center (PCC).

When you use the switch's IP address to log into the switch, the following screen displays:

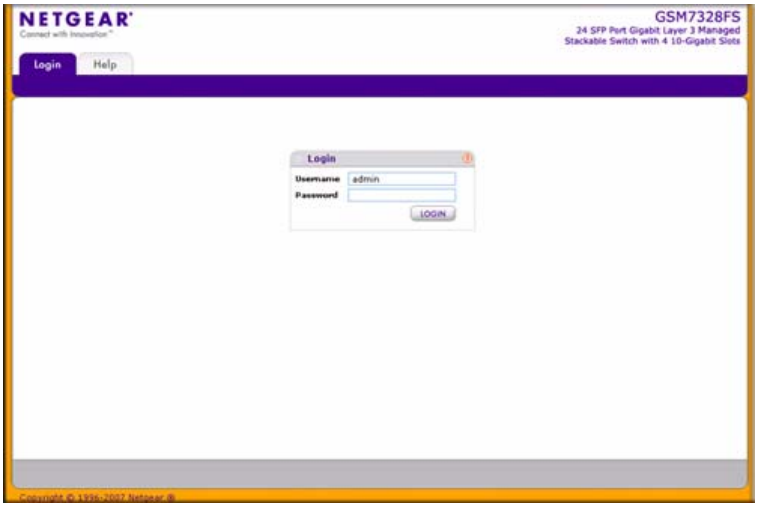


Figure 4-1

The switch can accommodate two types of users: administrative users and guests. An administrative user may configure the switch for network application, but a guest may not. The guest may only view the settings and status of the network. As shipped from the factory, both users can log in without a password. Netgear strongly recommends that the network administrator creates a unique password for the administrative user before placing the switch into production.

The following screen shows an example of the PCC:

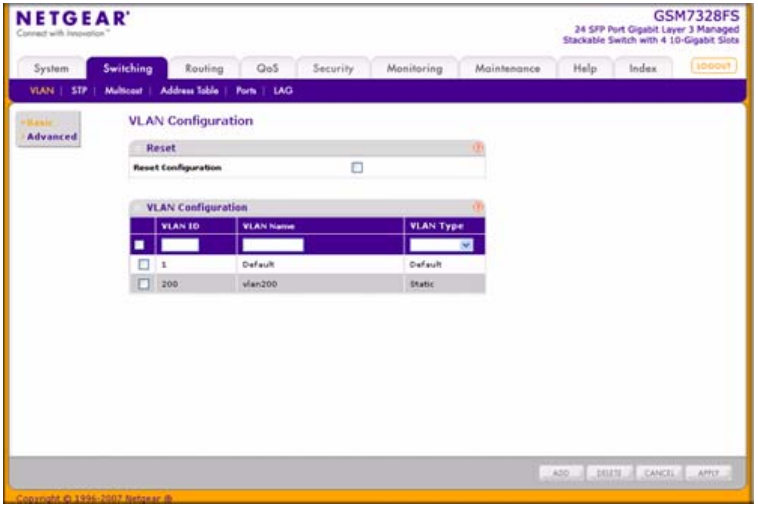


Figure 4-2

The new PCC web interface has the following four new significant features:

1. A layout change: The new layout organizes the navigation pane into two rows of tags, as shown in the following screen:

Figure 4-3

- Main Tags
  The PCC provides the following main tags:
  - System
    This tag contains configuration and status information for system features and services such as the timer, DNS server, IP address, and system resource usage.
  - Switching
    This tag contains features that relate to Layer 2 services such as VLANs, link aggregation, spanning tree protocol, port configuration, and the MAC address table.
  - Routing
    This tag contains Layer 3 services such as VLAN routing, port routing, and protocols such as RIP, OSPF, VRRP, and other protocols.
  - QoS
    This tag contains quality of service features such as DiffServ and CoS queue assignment.
  - Security
    This tag contains security services such as 802.1x port authentication, traffic control with various forwarding controls, and ACLs.
  - Monitoring
    This tag contains Ethernet port statistics, various system logs, and port mirroring.
  - Maintenance
    This tag contains services to perform a firmware upgrade, to save the configuration, and to perform a backup of the configuration.
  - Help
    This tag provides access to the Netgear product support Web site and the online user guide.

  - Index
    This tag contains the site index that allows direct access to any of the pages under the main tags and sub tags.

- Sub Tags
  The sub tag content changes depending on the selected main tag. In turn, each sub tag provides further sub categories of functions.

2. Unified Web Control Buttons
   Depending on the selected main tag and sub tag, in the lower right corner, there are buttons that enable you to perform various page-dependent operations:

   - Add
     Add a new class, group, ACL, or VLAN.
   - Apply
     Apply all changes that you made to a page.
   - Cancel
     Cancel all changes that you made to a page.
   - Delete
     Delete an existing list or group that was created by using an Add operation.
   - Refresh
     Refresh the data on the page such as log entry, port statistics, and other data.

3. Index Page
   One of the unique features of the PCC is the Index page. This page provides links to all available pages on the PCC, allowing you to connect to each page directly. On the Index page, you can use your Web browser's search function to locate a particular feature, and then connect directly to the page that enables you to view or configure that feature. Note that when you access a page directly from the Index page, the navigation pane does not adjust as it normally would when you navigate to the page by using a main tag and sub tag.

4. Save the Configuration
   When you click the Apply button to save the changes, the changes are applied to the switch but not saved into the permanent memory of the switch. When you reboot the switch, the changes are lost.To save the changes into the permanent memory of the switch, use the Save Configuration function that you can reach by clicking on the Maintenance tag and then on the Save Config tag.

Configuring an SNMP V3 User Profile

Configuring an SNMP V3 user profile is a part of user configuration. Any user can connect to the switch using the SNMPv3 protocol, but for authentication and encryption, additional steps are needed. Use the following steps to configure an SNMP V3 new user profile.

1. Select **System**>**Configuration**>**User Accounts** from the hierarchical tree on the left side of the web interface.
2. Using the **User** pulldown menu, select **Create** to create a new user.
3. Enter a new user name in the User Name field.
4. Enter a new user password in the Password field and then retype it in the Confirm Password field.

Note: If SNMPv3 Authentication is to be used for this user, the password must be eight or more alphanumeric characters.

5. If you do not need authentication, go to Step 9.
6. To enable authentication, use the **Authentication Protocol** pulldown menu to select either MD5 or SHA for the authentication protocol.
7. If you do not need encryption, go to Step 9.
8. To enable encryption, use the **Encryption Protocol** pulldown menu to select **DES** for the encryption scheme. Then, enter in the Encryption Key field an encryption code of eight or more alphanumeric characters.
9. Click **Submit**.

Chapter 5
Virtual LANs

Adding Virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security and management of multicast traffic.

A VLAN is a set of end stations and the switch ports that connect them. You may have many reasons for the logical division, such as department or project membership. The only physical requirement is that the end station and the port to which it is connected both belong to the same VLAN.

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station may omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet may either reject it or insert a tag using its default VLAN ID. A given port may handle traffic for more than one VLAN, but it can only support one default VLAN ID.

The Private Edge VLAN feature lets you set protection between ports located on the switch. This means that a protected port cannot forward traffic to another protected port on the same switch.

The feature does not provide protection between ports located on different switches.

VLAN Configuration Example

The diagram in this section shows a switch with four ports configured to handle the traffic for two VLANs. port 1/0/2 handles traffic for both VLANs, while port 1/0/1 is a member of VLAN 2 only, and ports 1/0/3 and 1/0/4 are members of VLAN 3 only. The script following the diagram shows the commands you would use to configure the switch as shown in the diagram.

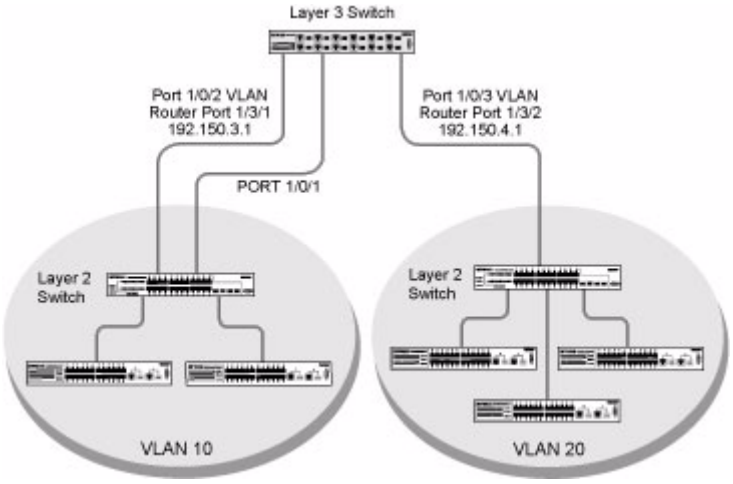


Figure 5-1

CLI Examples

The following examples show how to create VLANs, assign ports to the VLANs, and assign a VLAN as the default VLAN to a port.

Example #1: Create Two VLANs

Use the following commands to create two VLANs and to assign the VLAN IDs while leaving the names blank.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 2
(Netgear Switch) (Vlan)#vlan 3
(Netgear Switch) (Vlan)#exit
```

Example #2: Assign Ports to VLAN2

This sequence shows how to assign ports to VLAN2, specify that frames will always be transmitted tagged from all member ports, and that untagged frames will be rejected on receipt.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan participation include 2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan acceptframe vlanonly
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan pvid 2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#exit
(Netgear Switch) (Config)#vlan port tagging all 2
(Netgear Switch) (Config)#
```

Example #3: Assign Ports to VLAN3

This example shows how to assign the ports that will belong to VLAN 3, and to specify that untagged frames will be accepted on port 1/0/4.

Note that port 1/0/2 belongs to both VLANs and that port 1/0/1 can never belong to VLAN 3.

```
(Netgear Switch) (Config)#interface range 1/0/2-1/0/4
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#vlan participation include 3
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#exit
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#vlan acceptframe all
(Netgear Switch) (Interface 1/0/4)#exit
(Netgear Switch) (Config)#exit
```

Example #4: Assign VLAN3 as the Default VLAN

This example shows how to assign VLAN 3 as the default VLAN for port 1/0/2.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#vlan pvid 3
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Graphical User Interface

Use the following screens to perform the same configuration using the Graphical User Interface:

- **Switching --> VLAN--> Configuration**. To create the VLANs and specify port participation.
- **Switching --> VLAN --> Port Configuration.** To specify the handling of untagged frames on receipt, and whether frames will be transmitted tagged or untagged.

Chapter 6 Link Aggregation

This section includes instructions on configuring Link Aggregation using the Command Line Interface and the Graphical User Interface.

Link Aggregation (LAG) allows the switch to treat multiple physical links between two end-points as a single logical link. All of the physical links in a given LAG must operate in full-duplex mode at the same speed.

Link Aggregation can be used to directly connect two switches when the traffic between them requires high bandwidth and reliability, or to provide a higher bandwidth connection to a public network. LAG offers the following benefits:

- Increased reliability and availability -- if one of the physical links in the LAG goes down, traffic is dynamically and transparently reassigned to one of the other physical links.
- Better use of physical resources -- traffic can be load-balanced across the physical links.
- Increased bandwidth -- the aggregated physical links deliver higher bandwidth than each individual link.
- Incremental increase in bandwidth -- A physical upgrade could produce a 10-times increase in bandwidth; LAG produces a two- or five-times increase, useful if only a small increase is needed.

Management functions treat a LAG as if it were a single physical port.

You can include a LAG in a VLAN. You can configure more than one LAG for a given switch.

CLI Example

This section provides an example of configuring the software to support Link Aggregation (LAG) to a server and to a Layer 3 switch.

Figure 6-1 shows the example network.

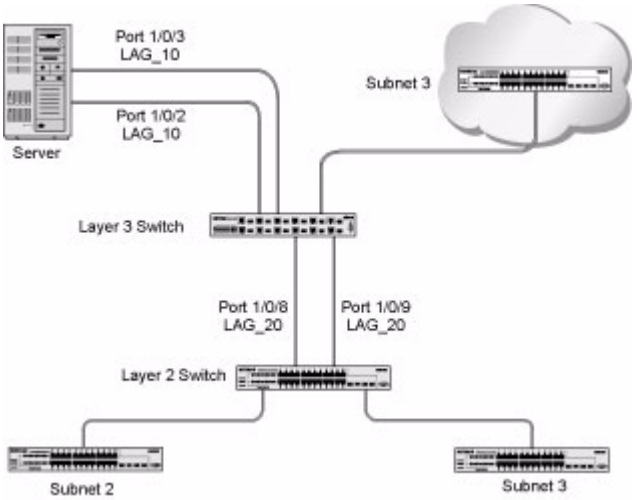


Figure 6-1

Example #1: Create two LAGS

```
(Netgear Switch) #config
(Netgear Switch) (Config)#port-channel lag_10
(Netgear Switch) (Config)#port-channel lag_20
(Netgear Switch) (Config)#exit
```

Use the **show port-channel all** command to show the logical interface ids you will use to identify the LAGs in subsequent commands. Assume that lag_10 is assigned id 1/1/1 and lag_20 is assigned id 1/1/2.

```
(Console) #show port-channel all

              Port-                    Link
Log.         Channel              Adm. Trap  STP            Mbr       Port     Port
Intf          Name         Link   Mode Mode  Mode    Type   Ports     Speed    Active
------ --------------- ------ ---- ---- ------ ------- ------ --------- ------
1/1/1     lag_10          Down    En.  En.  Dis.    Dynamic
1/1/2     lag_20          Down    En.  En.  Dis.    Dynamic
```

Example #2: Add the ports to the LAGs

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 0/2
(Netgear Switch) (Interface 0/2)#addport 1/1
(Netgear Switch) (Interface 0/2)#exit
(Netgear Switch) (Config)#interface 0/3
(Netgear Switch) (Interface 0/3)#addport 1/1
(Netgear Switch) (Interface 0/3)#exit
(Netgear Switch) (Config)#interface 0/8
(Netgear Switch) (Interface 0/8)#addport 1/2
(Netgear Switch) (Interface 0/8)#exit
(Netgear Switch) (Config)#interface 0/9
(Netgear Switch) (Interface 0/9)#addport 1/2
(Netgear Switch) (Interface 0/9)#exit
(Netgear Switch) (Config)#exit
```

Example #3: Enable both LAGs

By default, the system enables link trap notification

```
(Console) #config
(Console) (Config)#port-channel adminmode all
(Console) (Config)#exit
```

At this point, the LAGs could be added to VLANs.

Chapter 7
IP Routing Services

IP routing services are divided into five areas:

- Port Routing
- VLAN Routing
- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF) Protocol
- Proxy Address Resolution Protocol (ARP)

Port Routing

The first networks were small enough for the end stations to communicate directly. As networks grew, Layer 2 bridging was used to segregate traffic, a technology that worked well for unicast traffic, but had problems coping with large quantities of multicast packets. The next major development was routing, where packets were examined and redirected at Layer 3. End stations needed to know how to reach their nearest router, and the routers had to understand the network topology so that they could forward traffic. Although bridges tended to be faster than routers, using routers allowed the network to be partitioned into logical subnetworks, which restricted multicast traffic and also facilitated the development of security mechanisms.

An end station specifies the destination station's Layer 3 address in the packet's IP header, but sends the packet to the MAC address of a router. When the Layer 3 router receives the packet, it will minimally:

- Look up the Layer 3 address in its address table to determine the outbound port
- Update the Layer 3 header
- Recreate the Layer 2 header

The router's IP address is often statically configured in the end station, although the 7000 Series Managed Switch supports protocols such as DHCP that allow the address to be assigned dynamically. Likewise, you may assign some of the entries in the routing tables used by the router statically, but protocols such as RIP and OSPF allow the tables to be created and updated dynamically as the network configuration changes.

Port Routing Configuration

The 7000 Series Managed Switch always supports Layer 2 bridging, but Layer 3 routing must be explicitly enabled, first for the 7000 Series Managed Switch as a whole, and then for each port which is to participate in the routed network.

The configuration commands used in the example in this section enable IP routing on ports 1/0/2,1/0/3, and 1/0/5. The router ID will be set to the 7000 Series Managed Switch's management IP address, or to that of any active router interface if the management address is not configured.

After the routing configuration commands have been issued, the following functions will be active:

- IP Forwarding, responsible for forwarding received IP packets.
- ARP Mapping, responsible for maintaining the ARP Table used to correlate IP and MAC addresses. The table contains both static entries and entries dynamically updated based on information in received ARP frames.
- Routing Table Object, responsible for maintaining the common routing table used by all registered routing protocols.

You may then activate RIP or OSPF, used by routers to exchange route information, on top of IP Routing. RIP is more often used in smaller networks, while OSPF was designed for larger and more complex topologies.

CLI Examples

This diagram shows a Layer 3 switch configured for port routing. It connects three different subnets, each connected to a different port. The script shows the commands you would use to configure a 7000 Series Managed Switch to provide the port routing support shown in the diagram.

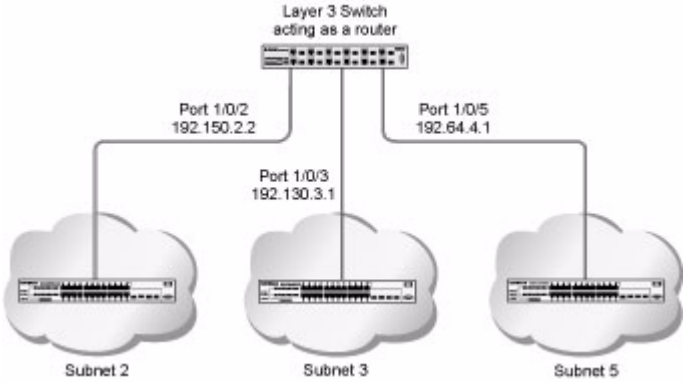


Figure 7-1

Example #1: Enabling routing for the Switch

Use the following command to enable routing for the switch. Execution of the command enables IP forwarding by default.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

Example #2: Enabling Routing for Ports on the Switch

Use the following commands to enable routing for ports on the switch. The default link-level encapsulation format is Ethernet. Configure the IP addresses and subnet masks for the ports. Network directed broadcast frames will be dropped and the maximum transmission unit (MTU) size will be 1500 bytes.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit

(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#routing
(Netgear Switch) (Interface 1/0/5)#ip address 192.150.5.1 255.255.255.0
(Netgear Switch) (Interface 1/0/5)#exit
(Netgear Switch) (Config)#exit
```

VLAN Routing

You can configure 7000 Series Managed Switch with some ports supporting VLANs and some supporting routing. You can also configure it to allow traffic on a VLAN to be treated as if the VLAN were a router port.

When a port is enabled for bridging (the default) rather than routing, all normal bridge processing is performed for an inbound packet, which is then associated with a VLAN. Its MAC Destination Address (DA) and VLAN ID are used to search the MAC address table. If routing is enabled for the VLAN and the MAC DA of an inbound unicast packet is that of the internal bridge-router interface, the packet will be routed. An inbound multicast packet will be forwarded to all ports in the VLAN, plus the internal bridge-router interface if it was received on a routed VLAN.

Since a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port, or for a subset. VLAN Routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans multiple physical networks, or when additional segmentation or security is required.

The next section will show you how to configure the 7000 Series Managed Switch to support VLAN routing and how to use RIP and OSPF. A port may be either a VLAN port or a router port, but not both. However, a VLAN port may be part of a VLAN that is itself a router port.

VLAN Routing Configuration

This section provides an example of how to configure 7000 Series Managed Switch to support VLAN routing. The configuration of the VLAN router port is similar to that of a physical port. The main difference is that, after the VLAN has been created, you must use the **show ip vlan** command to determine the VLAN's interface ID so that you can use it in the router configuration commands.

CLI Examples

The diagram in this section shows a Layer 3 switch configured for port routing. It connects two VLANs, with two ports participating in one VLAN, and one port in the other. The script shows the commands you would use to configure a 7000 Series Managed Switch to provide the VLAN routing support shown in the diagram.

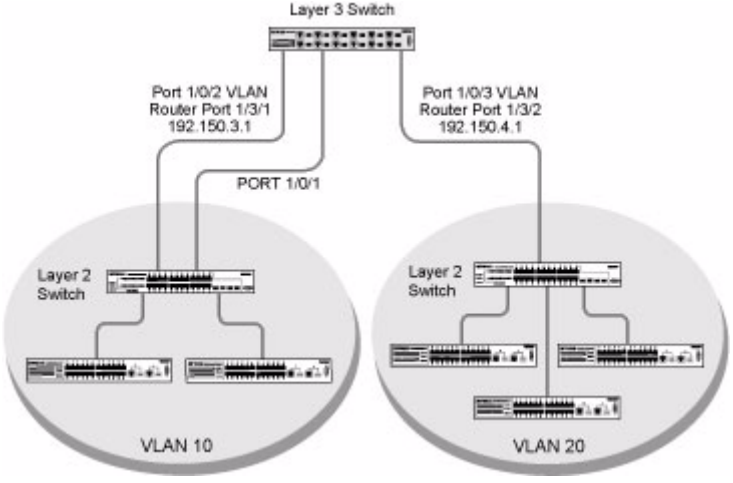


Figure 7-2

Example #1: Create Two VLANs

The following code sequence shows an example of creating two VLANs with egress frame tagging enabled.

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#vlan 20
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #conf
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan participation include 10
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan pvid 10
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#vlan participation include 20
(Netgear Switch) (Interface 1/0/3)#vlan pvid 20
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#vlan port tagging all 10
(Netgear Switch) (Config)#vlan port tagging all 20
(Netgear Switch) (Config)#exit
```

Example #2: Set Up VLAN Routing for the VLANs and the Switch.

The following code sequence shows how to enable routing for the VLANs:

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan routing 10
(Netgear Switch) (Vlan)#vlan routing 20
(Netgear Switch) (Vlan)#exit
```

This returns the logical interface IDs that will be used instead of slot/port in subsequent routing commands. Assume that VLAN 10 is assigned ID 3/1 and VLAN 20 is assigned ID 3/2.

Enable routing for the switch:

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

The next sequence shows an example of configuring the IP addresses and subnet masks for the virtual router ports.

```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface-vlan 10)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface-vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface-vlan 20)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface-vlan 20)#exit
(Netgear Switch) (Config)#exit
```

VLAN Routing RIP Configuration

Routing Information Protocol (RIP) is one of the protocols which may be used by routers to exchange network topology information. It is characterized as an “interior” gateway protocol, and is typically used in small to medium-sized networks.

A router running RIP will send the contents of its routing table to each of its adjacent routers every 30 seconds. When a route is removed from the routing table it will be flagged as unusable by the receiving routers after 180 seconds, and removed from their tables after an additional 120 seconds.

There are two versions of RIP:

- RIPv1 defined in RFC 1058
  - Routes are specified by IP destination network and hop count
  - The routing table is broadcast to all stations on the attached network
- RIPv2 defined in RFC 1723
  - Route specification is extended to include subnet mask and gateway
  - The routing table is sent to a multicast address, reducing network traffic
  - An authentication method is used for security

The 7000 Series Managed Switch supports both versions of RIP. You may configure a given port:

- To receive packets in either or both formats
- To transmit packets formatted for RIPv1 or RIPv2 or to send RIPv2 packets to the RIPv1 broadcast address
- To prevent any RIP packets from being received
- To prevent any RIP packets from being transmitted.

CLI Example

This example adds support for RIPv2 to the configuration created in the base VLAN routing example. A second router, using port routing rather than VLAN routing, has been added to the network.

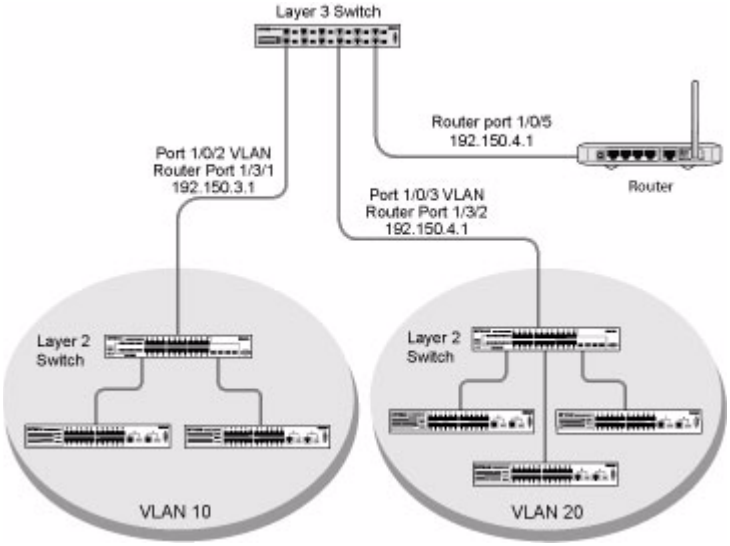


Figure 7-3

Example of configuring VLAN Routing with RIP support on a 7000 Series Managed Switch

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#vlan 20
(Netgear Switch) (Vlan)#vlan routing 10
(Netgear Switch) (Vlan)#vlan routing 20
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #conf
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#vlan port tagging all 10
(Netgear Switch) (Config)#vlan port tagging all 20
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#vlan participation include 10
(Netgear Switch) (Interface 1/0/2)#vlan pvid 10
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#vlan participation include 20
(Netgear Switch) (Interface 1/0/3)#vlan pvid 20
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface vlan 20)#exit

Enable RIP for the switch. The route preference will default to 15.
(Netgear Switch) (Config)#router rip
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#exit

Configure the IP address and subnet mask for a non-virtual router port.
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#ip address 192.150.5.1 255.255.255.0
(Netgear Switch) (Interface 1/0/5)#exit

Enable RIP for the VLAN router ports. Authentication will default to none, and
no default route entry will be created.
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip rip
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip rip
(Netgear Switch) (Interface vlan 20)#exit
(Netgear Switch) (Config)#exit
```

VLAN Routing OSPF Configuration

For larger networks Open Shortest Path First (OSPF) is generally used in preference to RIP. OSPF offers several benefits to the administrator of a large and/or complex network:

- Less network traffic:
  - Routing table updates are sent only when a change has occurred
  - Only the part of the table which has changed is sent
  - Updates are sent to a multicast, not a broadcast, address
- Hierarchical management, allowing the network to be subdivided

The top level of the hierarchy of an OSPF network is known as an autonomous system (AS) or routing domain, and is a collection of networks with a common administration and routing strategy. The AS is divided into areas: intra-area routing is used when a source and destination address are in the same area, and inter-area routing across an OSPF backbone is used when they are not. An inter-area router communicates with border routers in each of the areas to which it provides connectivity.

The 7000 Series Managed Switch operating as a router and running OSPF will determine the best route using the assigned cost and the type of the OSPF route. The order for choosing a route if more than one type of route exists is as follows:

- Intra-area
- Inter-area
- External type 1: the route is external to the AS
- External Type 2: the route was learned from other protocols such as RIP

CLI Example

This example adds support for OSPF to the configuration created in the base VLAN routing example. The script shows the commands you would use to configure the 7000 Series Managed Switch as an inter-area router. Refer to Figure 7-2.

Example of configuring OSPF on a 7000 Series Managed Switch acting as an inter-area router:

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#vlan 20
(Netgear Switch) (Vlan)#vlan routing 10
(Netgear Switch) (Vlan)#vlan routing 20
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #conf
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#vlan port tagging all 10
(Netgear Switch) (Config)#vlan port tagging all 20
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#vlan participation include 10
(Netgear Switch) (Interface 1/0/2)#vlan pvid 10
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#vlan participation include 20
(Netgear Switch) (Interface 1/0/3)#vlan pvid 20
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface vlan 20)#exit

Specify the router ID and enable OSPF for the switch.
(Netgear Switch) (Config)#router ospf
(Netgear Switch) (Config router)#router-id 192.150.9.9
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#exit

Enable OSPF for the VLAN and physical router ports.
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface vlan 10)#ip ospf
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip ospf areaid 0.0.0.3
(Netgear Switch) (Interface vlan 20)#ip ospf
(Netgear Switch) (Interface vlan 20)#exit
```

```
Set the OSPF priority and cost for the VLAN and physical router ports.
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip ospf priority 128
(Netgear Switch) (Interface vlan 10)#ip ospf cost 32
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip ospf priority 255
(Netgear Switch) (Interface vlan 20)#ip ospf cost 64
(Netgear Switch) (Interface vlan 20)#exit
(Netgear Switch) (Config)#exit
```

Routing Information Protocol

Routing Information Protocol (RIP) is one of the protocols which may be used by routers to exchange network topology information. It is characterized as an “interior” gateway protocol, and is typically used in small to medium-sized networks.

RIP Configuration

A router running RIP will send the contents of its routing table to each of its adjacent routers every 30 seconds. When a route is removed from the routing table it will be flagged as unusable by the receiving routers after 180 seconds, and removed from their tables after an additional 120 seconds.

There are two versions of RIP:

- RIPv1 defined in RFC 1058
  - Routes are specified by IP destination network and hop count
  - The routing table is broadcast to all stations on the attached network
- RIPv2 defined in RFC 1723
  - Route specification is extended to include subnet mask and gateway
  - The routing table is sent to a multicast address, reducing network traffic
  - An authentication method is used for security

The 7000 Series Managed Switch supports both versions of RIP. You may configure a given port:

- To receive packets in either or both formats
- To transmit packets formatted for RIPv1 or RIPv2 or to send RIPv2 packets to the RIPv1 broadcast address
- To prevent any RIP packets from being received

- To prevent any RIP packets from being transmitted

CLI Examples

The configuration commands used in the following example enable RIP on ports 1/0/2 and 1/0/3 as shown in the network illustrated in Figure 7-4

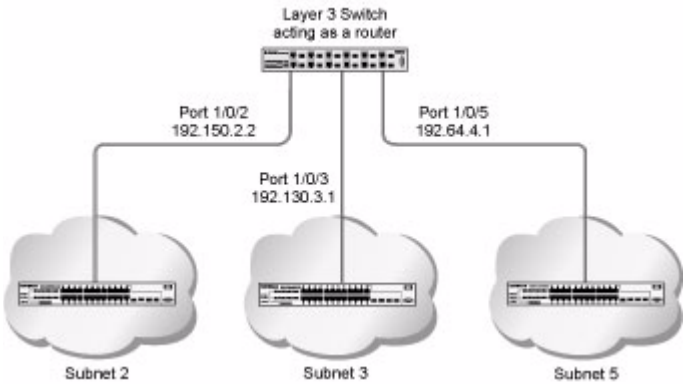


Figure 7-4

Example #1: Enable Routing for the Switch

The following sequence enables routing for the switch:

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

Example #2: Enable Routing for Ports

The following command sequence enables routing and assigns IP addresses for ports 1/0/2 and 1/0/3.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#exit
```

Example #3: Enable RIP for the Switch

The next sequence enables RIP for the switch. the route preference defaults to 15.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#router rip
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#exit
(Netgear Switch) (Config)#exit
```

Example #4: Enable RIP for ports 1/0/2 and 1/0/3

This command sequence enables RIP for ports 1/0/2 and 1/0/3. Authentication defaults to none, and no default route entry is created. The commands specify that both ports receive both RIPv1 and RIPv2 frames, but send only RIPv2 formatted frames.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip rip
(Netgear Switch) (Interface 1/0/2)#ip rip receive version both
(Netgear Switch) (Interface 1/0/2)#ip rip send version rip2
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip rip
(Netgear Switch) (Interface 1/0/3)#ip rip receive version both
(Netgear Switch) (Interface 1/0/3)#ip rip send version rip2
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#exit
```

OSPF

For larger networks Open Shortest Path First (OSPF) is generally used in preference to RIP. OSPF offers several benefits to the administrator of a large and/or complex network:

- Less network traffic:
  - Routing table updates are sent only when a change has occurred
  - Only the part of the table which has changed is sent
  - Updates are sent to a multicast, not a broadcast, address
- Hierarchical management, allowing the network to be subdivided

The top level of the hierarchy of an OSPF network is known as an autonomous system (AS) or routing domain, and is a collection of networks with a common administration and routing strategy. The AS is divided into areas: intra-area routing is used when a source and destination address are in the same area, and inter-area routing across an OSPF backbone is used when they are not. An inter-area router communicates with border routers in each of the areas to which it provides connectivity.

The 7000 Series Managed Switch operating as a router and running OSPF will determine the best route using the assigned cost and the type of the OSPF route. The order for choosing a route if more than one type of route exists is as follows:

- Intra-area
- Inter-area
- External type 1: the route is external to the AS
- External Type 2: the route was learned from other protocols such as RIP

CLI Examples

The examples in this section show you how to configure a 7000 Series Managed Switch first as an inter-area router and then as a border router. They show two areas, each with its own border router connected to one inter-area router.

The first diagram shows a network segment with an inter-area router connecting areas 0.0.0.2 and 0.0.0.3. The example script shows the commands used to configure a 7000 Series Managed Switch as the inter-area router in the diagram by enabling OSPF on port 1/0/2 in area 0.0.0.2 and port 1/0/3 in area 0.0.0.3.

Example #1: Configuring an Inter-Area Router

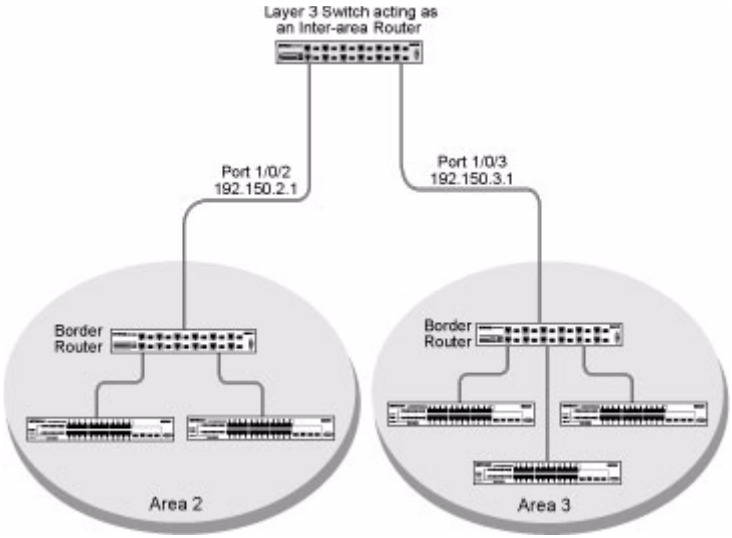


Figure 7-5

Enable Routing for the Switch. The following command sequence enables ip routing for the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

Assign IP Addresses for Ports. The following sequence enables routing and assigns IP addresses for ports 1/0/2 and 1/0/3:

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#exit
```

Specify Router ID and Enable OSPF for the Switch. The following sequence specifies the router ID and enables OSPF for the switch. Set disable1583 compatibility to prevent the routing loop.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#router ospf
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#router-id 192.150.9.9
(Netgear Switch) (Config router)#no 1583compatibility
(Netgear Switch) (Config router)#exit
(Netgear Switch) (Config)#exit
```

Enable and Configure OSPF for the Ports. The following sequence enables OSPF and sets the OSPF priority and cost for the ports.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip ospf
(Netgear Switch) (Interface 1/0/2)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/2)#ip ospf priority 128
(Netgear Switch) (Interface 1/0/2)#ip ospf cost 32
(Netgear Switch) (Interface 1/0/2)#exit

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip ospf
(Netgear Switch) (Interface 1/0/3)#ip ospf areaid 0.0.0.3
(Netgear Switch) (Interface 1/0/3)#ip ospf priority 255
(Netgear Switch) (Interface 1/0/3)#ip ospf cost 64
(Netgear Switch) (Interface 1/0/3)#exit(Netgear Switch) (Config)#exit
```

Example #2: Configuring OSPF on a Border Router

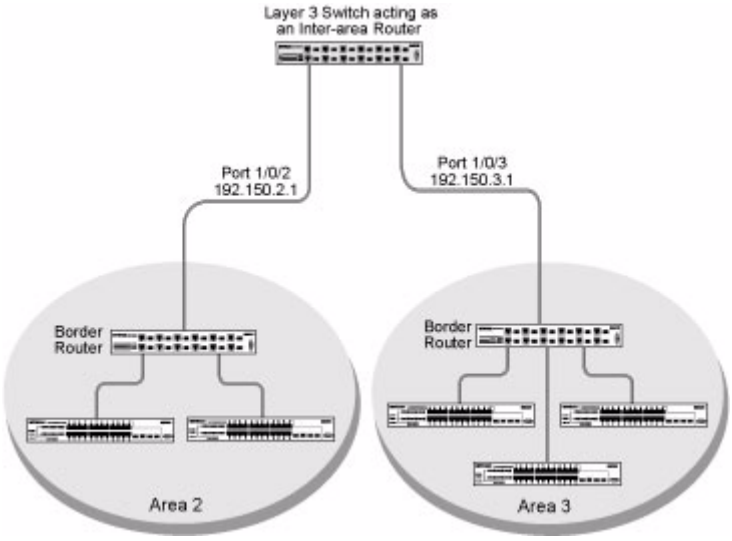


Figure 7-6

The following example configures OSPF on a 7000 Series Managed Switch operating as a border router:

```
Enable routing for the switch.

(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing

Enable routing & assign IP for ports 1/0/2, 1/0/3 and 1/0/4.

(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.2 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.130.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#routing
(Netgear Switch) (Interface 1/0/4)#ip address 192.64.4.1 255.255.255.0
(Netgear Switch) (Interface 1/0/4)#exit

Specify the router ID and enable OSPF for the switch. Set disable
1583compatibility to prevent a routing loop.

(Netgear Switch) (Config)#router ospf
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#router-id 192.130.1.1
(Netgear Switch) (Config router)#no 1583compatibility
(Netgear Switch) (Config router)#exit
(Netgear Switch) (Config)#exit
```

```
Enable OSPF for the ports and set the OSPF priority and cost for the ports.

(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip ospf
(Netgear Switch) (Interface 1/0/2)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/2)#ip ospf priority 128
(Netgear Switch) (Interface 1/0/2)#ip ospf cost 32
(Netgear Switch) (Interface 1/0/2)#exit

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip ospf
(Netgear Switch) (Interface 1/0/3)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/3)#ip ospf priority 255
(Netgear Switch) (Interface 1/0/3)#ip ospf cost 64
(Netgear Switch) (Interface 1/0/3)#exit

(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#ip ospf
(Netgear Switch) (Interface 1/0/4)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/4)#ip ospf priority 255
(Netgear Switch) (Interface 1/0/4)#ip ospf cost 64
(Netgear Switch) (Interface 1/0/4)#exit
(Netgear Switch) (Config)#exit
```

Proxy Address Resolution Protocol (ARP)

This section describes the Proxy Address Resolution Protocol (ARP) feature.

Overview

- Proxy ARP allows a router to answer ARP requests where the target IP address is not the router itself but a destination that the router can reach
- If a host does not know the default gateway, proxy ARP can learn the first hop
- Machines in one physical network appear to be part of another logical network
- Without proxy ARP, a router will only respond to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived

CLI Examples

The following are examples of the commands used in the proxy ARP feature.

Example #1: show ip interface

```
(Netgear Switch) #show ip interface ?

<slot/port>              Enter an interface in slot/port format.
brief                    Display summary information about IP configuration
                         settings for all ports.

(Netgear Switch) #show ip interface 0/24

Routing Mode..................................... Disable
Administrative Mode.............................. Enable
Forward Net Directed Broadcasts.................. Disable
Proxy ARP........................................ Disable
Active State..................................... Inactive
Link Speed Data Rate............................. Inactive
MAC Address...................................... 08:00:17:05:05:02
Encapsulation Type............................... Ethernet
IP MTU........................................... 1500
```

Example #2: ip proxy-arp

```
(Netgear Switch) (Interface 0/24)#ip proxy-arp ?

<cr>                     Press Enter to execute the command.

(Netgear Switch) (Interface 0/24)#ip proxy-arp
```

Chapter 8
Virtual Router Redundancy Protocol

When an end station is statically configured with the address of the router that will handle its routed traffic, a single point of failure is introduced into the network. If the router goes down, the end station is unable to communicate. Since static configuration is a convenient way to assign router addresses, Virtual Router Redundancy Protocol (VRRP) was developed to provide a backup mechanism.

VRRP eliminates the single point of failure associated with static default routes by enabling a backup router to take over from a “master” router without affecting the end stations using the route. The end stations will use a “virtual” IP address that will be recognized by the backup router if the master router fails. Participating routers use an election protocol to determine which router is the master router at any given time. A given port may appear as more than one virtual router to the network, also, more than one port on a 7000 Series Managed Switch may be configured as a virtual router. Either a physical port or a routed VLAN may participate.

CLI Examples

This example shows how to configure the 7000 Series Managed Switch to support VRRP. Router 1 will be the default master router for the virtual route, and Router 2 will be the backup router.

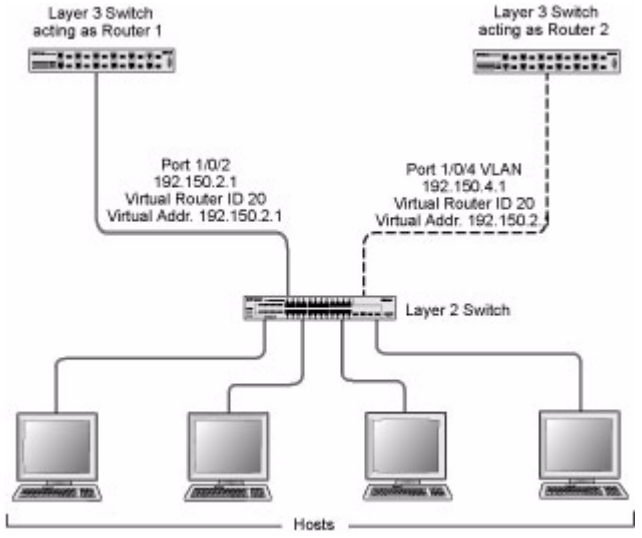


Figure 8-1

Example #1: Configure VRRP on a Master Router

The following is an example of configuring VRRP on a 7000 Series Managed Switch acting as the master router:

```
              Enable routing for the switch. IP forwarding will then be enabled
              by default.
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing

              Configure the IP addresses and subnet masks for the port that will
              particpate in the protocol.
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit

              Enable VRRP for the switch.
(Netgear Switch) (Config)#ip vrrp

              Assign virtual router IDs to the port that will particpate in the
              protocol.
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip vrrp 20

              Specify the IP address that the virtual router function will rec-
              ognize. Note that the virtual IP address on port 1/0/2 is the same
              as the port's actual IP address, therefore this router will always
              be the VRRP master when it is active. And the priority default is
              255.
(Netgear Switch) (Interface 1/0/2)#ip vrrp 20 ip 192.150.2.1

              Enable VRRP on the port.
(Netgear Switch) (Interface 1/0/2)#ip vrrp 20 mode
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Example #2: Configure VRRP on a Backup Router

The following is an example of configuring VRRP on a 7000 Series Managed Switch acting as the backup router:

```
              Enable routing for the switch. IP forwarding will then be enabled
              by default.
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing

              Configure the IP addresses and subnet masks for the port that will
              particpate in the protocol.
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#routing
(Netgear Switch) (Interface 1/0/4)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface 1/0/4)#exit

              Enable VRRP for the switch.
(Netgear Switch) (Config)#ip vrrp 20

              Assign virtual router IDs to the port that will particpate in the
              protocol.
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20

              Specify the IP address that the virtual router function will rec-
              ognize. Since the virtual IP address on port 1/0/4 is the same as
              Router 1's port 1/0/2 actual IP address, this router will always
              be the VRRP backup when Router 1 is active.
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20 ip 192.150.2.1

              Set the priority for the port. The default priority is 100.
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20 priority 254

              Enable VRRP on the port.
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20 mode
(Netgear Switch) (Interface 1/0/4)#exit
(Netgear Switch) (Config)#exit
```

Chapter 9
Access Control Lists (ACLs)

This section describes the Access Control Lists (ACLs) feature.

Overview

Access Control Lists (ACLs) can control the traffic entering a network. Normally ACLs reside in a firewall router or in a router connecting two internal networks. When you configure ACLs, you can selectively admit or reject inbound traffic, thereby controlling access to your network or to specific resources on your network.

You can set up ACLs to control traffic at Layer 2, or Layer3. MAC ACLs are used for Layer 2. IP ACLs are used for Layers 3.

Each ACL contains a set of rules that apply to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and may apply to one or more of the fields within a packet.

Limitations

The following limitations apply to ACLs. These limitations are platform dependent.

- Maximum of 100 ACLs
- Maximum rules per ACL is 8-10
- Stacking systems do not support redirection

The system does not support MAC ACLs and IP ACLs on the same interface.

The system supports ACLs set up for inbound traffic only.

MAC ACLs

MAC ACLs are Layer 2 ACLs. You can configure the rules to inspect the following fields of a packet (limited by platform):

- Source MAC address with mask

- Destination MAC address with mask
- VLAN ID (or range of IDs)
- Class of Service (CoS) (802.1p)
- Ethertype
- L2 ACLs can apply to one or more interfaces
- Multiple access lists can be applied to a single interface - sequence number determines the order of execution
- You cannot configure a MAC ACL and an IP ACL on the same interface
- You can assign packets to queues using the assign queue option
- You can redirect packets using the redirect option

Configuring IP ACLs

IP ACLs classify for Layer 3.

Each ACL is a set of up to ten rules applied to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and may apply to one or more of the following fields within a packet:

- Source IP address
- Destination IP address
- Source Layer 4 port
- Destination Layer 4 port
- ToS byte
- Protocol number

Note that the order of the rules is important: when a packet matches multiple rules, the first rule takes precedence. Also, once you define an ACL for a given port, all traffic not specifically permitted by the ACL will be denied access.

Process

To configure ACLs, follow these steps:

- Create an ACL by specifying a name (MAC ACL) or a number (IP ACL)
- Add new rules to the ACL
- Configure the match criteria for the rules
- Apply the ACL to one or more interfaces

IP ACL Examples

Example #1: Set up an IP ACL with Two Rules

The script in this section shows you how to set up an IP ACL with two rules, one applicable to TCP traffic and one to UDP traffic. The content of the two rules is the same. TCP and UDP packets will only be accepted by the 7000 Series Managed Switch if the source and destination stations have IP addresses that fall within the defined sets.

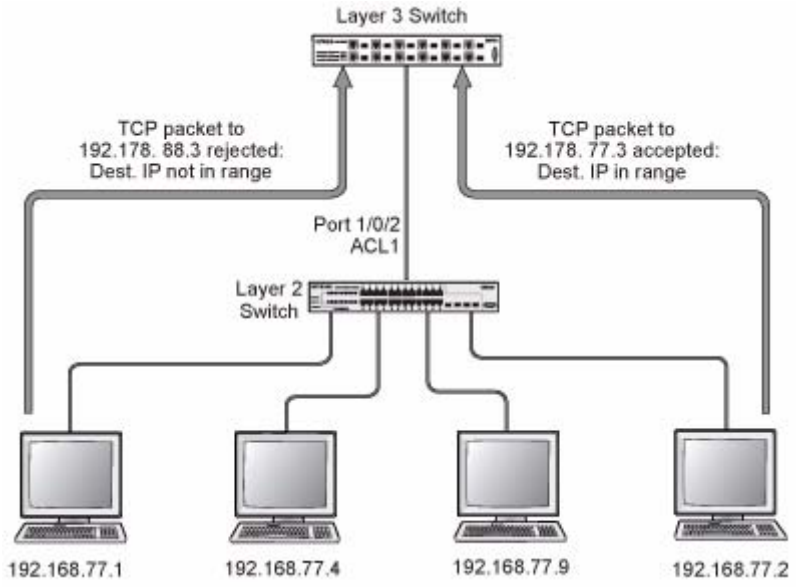


Figure 9-1

The following is an example of configuring ACL support on a 7000 Series Managed Switch.

```
Create ACL 101. Define the first rule: the ACL will permit packets with a match
on the specified source IP address (after the mask has been applied), that are
carrying TCP traffic, and that are sent to the specified destination IP address.
(Netgear Switch) #config
(Netgear Switch) (Config)#access-list 101 permit tcp 192.168.77.0 0.0.0.255
192.178.77.0 0.0.0.255

Define the second rule for ACL 101. Define the rule to set similar conditions
for UDP traffic as for TCP traffic.
(Netgear Switch) (Config)#access-list 101 permit udp 192.168.77.0 0.0.0.255
192.178.77.0 0.0.0.255

Apply the rule to inbound traffic on port 1/0/2. Only traffic matching the
criteria will be accepted.
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip access-group 101 in
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Example #2: Configure a One-Way Access Using a TCP Flag in an ACL

This example shows how to set up one-way web access using a TCP flag in an ACL.

PC1 can access FTP server1 and FTP server2 but PC2 only access FTP server2.

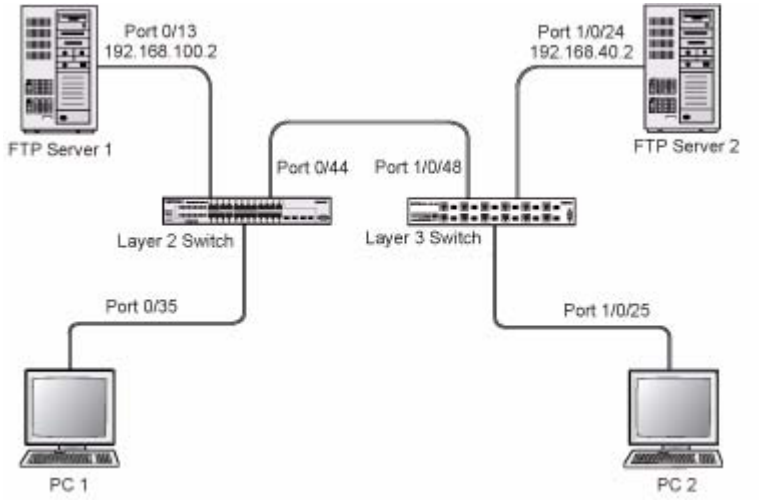


Figure 9-2

The example is shown as CLI commands and as a Web interface procedure.

CLI Commands

To use the CLI to configure the GSM7248R, enter the following CLI commands:

Step 1: Configure the GSM7248R (see Figure 9-2)

```
Create VLAN 30 with port 0/3 and assign IP address 192.168.30.1/24.
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 30
(Netgear Switch) (Vlan)#vlan routing 30
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 0/35
(Netgear Switch) (Interface 0/35)#vlan pvid 30
(Netgear Switch) (Interface 0/35)#vlan participation include 30
(Netgear Switch) (Interface 0/35)#exit
(Netgear Switch) (Config)#interface vlan 30
(Netgear Switch) (Interface-vlan 30)#routing
(Netgear Switch) (Interface-vlan 30)#ip address 192.168.30.1 255.255.255.0
(Netgear Switch) (Interface-vlan 30)#exit
(Netgear Switch) (Config)#exit

Create VLAN 100 with port 0/13 and assign IP address 192.168.100.1/24.
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 100
(Netgear Switch) (Vlan)#vlan routing 100
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 0/13
(Netgear Switch) (Interface 0/13)#vlan pvid 100
(Netgear Switch) (Interface 0/13)#vlan participation include 100
(Netgear Switch) (Interface 0/13)#exit
(Netgear Switch) (Config)#interface vlan 100
(Netgear Switch) (Interface-vlan 100)#routing
(Netgear Switch) (Interface-vlan 100)#ip address 192.168.100.1 255.255.255.0
(Netgear Switch) (Interface-vlan 100)#exit
(Netgear Switch) (Config)#exit
```

```
Create VLAN 200 with port 0/44 and assign IP address 192.168.200.1/24.
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#vlan routing 200
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 0/44
(Netgear Switch) (Interface 0/44)#vlan pvid 200
(Netgear Switch) (Interface 0/44)#vlan participation include 200
(Netgear Switch) (Interface 0/44)#exit
(Netgear Switch) (Config)#interface vlan 200
(Netgear Switch) (Interface-vlan 200)#routing
(Netgear Switch) (Interface-vlan 200)#ip address 192.168.200.1 255.255.255.0
(Netgear Switch) (Interface-vlan 200)#exit

Add two static routes so that the switch forwards the packets for which the
destinations are 192.168.40.0/24 and 192.168.50.0/24 to the correct next hops.
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip route 192.168.40.0 255.255.255.0 192.168.200.2
(Netgear Switch) (Config)#ip route 192.168.50.0 255.255.255.0 192.168.200.2

Create an ACL that denies all the packets with TCP flags +syn-ack.
(Netgear Switch) (Config)#access-list 101 deny tcp any any flag +syn -ack

Create an ACL that permits all the IP packets.
(Netgear Switch) (Config)#access-list 102 permit ip any any

Apply the ACL 101 and 102 to the port 0/44; the sequence of 101 is 1 and
of 102 is 2.
(Netgear Switch) (Config)#interface 0/44
(Netgear Switch) (Interface 0/44)#ip access-group 101 in 1
(Netgear Switch) (Interface 0/44)#ip access-group 102 in 2
(Netgear Switch) (Interface 0/44)#exit
```

To use the CLI to Configure the GSM7352S, enter the following CLI commands:

Step 2: Configure the GSM7352S (see Figure 9-2)

```
Create VLAN 40 with port 1/0/24 and assign IP address 192.168.40.1/24.
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 40
(Netgear Switch) (Vlan)#vlan routing 40
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 40
(Netgear Switch) (Interface 1/0/24)#vlan participation include 40
(Netgear Switch) (Interface 1/0/24)#exit
(Netgear Switch) (Config)#interface vlan 40
(Netgear Switch) (Interface-vlan 40)#routing
(Netgear Switch) (Interface-vlan 40)#ip address 192.168.40.1 255.255.255.0
(Netgear Switch) (Interface-vlan 40)#exit

Create VLAN 50 with port 1/0/25 and assign IP address 192.168.50.1/24.
(Netgear Switch)(Config)#exit
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 50
(Netgear Switch) (Vlan)#vlan routing 50
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/25
(Netgear Switch) (Interface 1/0/25)#vlan pvid 50
(Netgear Switch) (Interface 1/0/25)#vlan participation include 50
(Netgear Switch) (Interface 1/0/25)#exit
(Netgear Switch) (Config)#interface vlan 50
(Netgear Switch) (Interface-vlan 50)#routing
(Netgear Switch) (Interface-vlan 50)#ip address 192.168.50.1 255.255.255.0
(Netgear Switch) (Interface-vlan 50)#exit
(Netgear Switch) (Config)#exit

Create VLAN 200 with port 1/0/48 and assign IP address 192.168.200.1/24.
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#vlan routing 200
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan pvid 200
(Netgear Switch) (Interface 1/0/48)#vlan participation include 200
(Netgear Switch) (Interface 1/0/48)#exit
(Netgear Switch) #interface vlan 200
(Netgear Switch) (Interface-vlan 200)#routing
(Netgear Switch) (Interface-vlan 200)#ip address 192.168.200.2 255.255.255.0
(Netgear Switch) (Interface-vlan 200)#exit
```

```
Add two static routes so that the switch forwards the packets with destinations
192.168.100.0/24 and 192.168.30.0/24 to the correct next hops.
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip route 192.168.100.0 255.255.255.0 192.168.200.1
(Netgear Switch) (Config)#ip route 192.168.30.0 255.255.255.0 192.168.200.1
```

Web Interface Procedure

To use the Web interface to configure the GSM7248R, proceed as follows:

1. Create VLAN 30 with IP address 192.168.30.1/24:

a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.

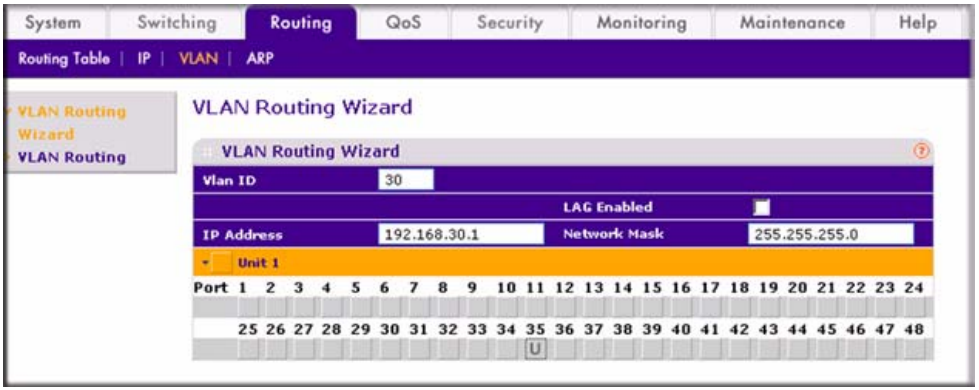


Figure 9-3

b. Enter the following information in the VLAN Routing Wizard:

- In the Vlan ID field, enter **30**.
- In the IP Address field, enter **192.168.30.1**.
- In the Network Mask field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port 35 twice until **U** displays. The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 30.

2. Create VLAN 100 with IP address 192.168.100.1/24:

   a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.

Figure 9-4

   b. Enter the following information in the VLAN Routing Wizard:

      - In the Vlan ID field, enter **100**.
      - In the IP Address field, enter **192.168.100.1**.
      - In the Network Mask field, enter **255.255.255.0**.

   c. Click **Unit 1**. The ports display.

   d. Click the gray box under port 13 twice until **U** displays. The U specifies that the egress packet is untagged for the port.

   e. Click **Apply** to save VLAN 100.

3. Create VLAN 200 with IP address 192.168.200.1/24:

a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.

Figure 9-5

b. Enter the following information in the VLAN Routing Wizard:

- In the Vlan ID field, enter **200**.
- In the IP Address field, enter **192.168.200.1**.
- In the Network Mask field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port 44 twice until **U** displays. The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 200.

4. Enable IP Routing:

   a. From the main menu, select Routing > IP > Basic > IP Configuration. A screen similar to the following displays.

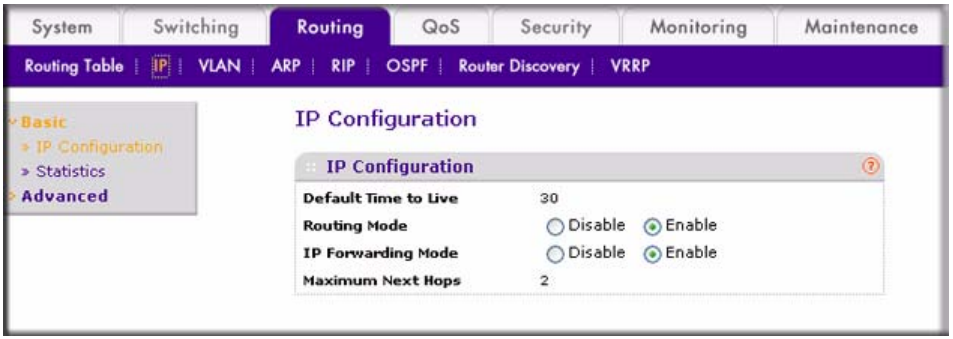


Figure 9-6

   b. Under IP Configuration, make the following selections:

   - Next to Routing Mode, select the **Enable** radio button.
   - Next to IP Forwarding Mode, select the **Enable** radio button.

   c. Click **Apply** to enable IP Routing.

5. Add a static route with IP address 192.268.40.0/24:

   a. From the main menu, select Routing > Routing Table > Basic > Route Configuration. A screen similar to the following displays.

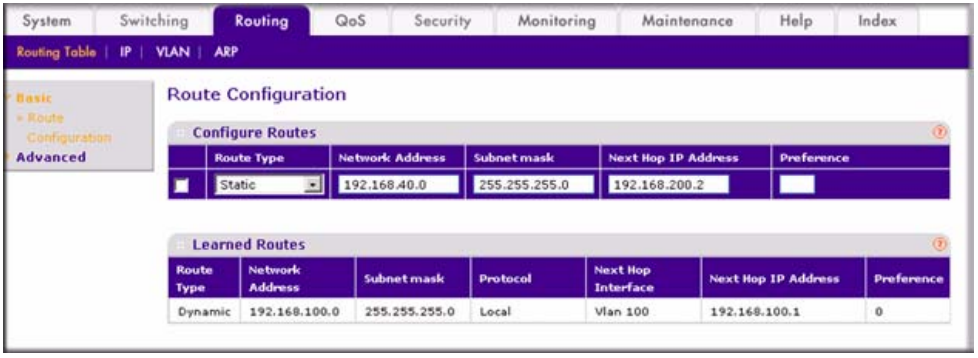


Figure 9-7

b. Under Configure Routes, make the following selection and enter the following information:

- Select **Static** from the Route Type pulldown menu.
- In the Network Address field, enter **192.168.40.0**.
- In the Subnet Mask field, enter **255.255.255.0**.
- In the Next Hop IP Address field, enter **192.168.200.2**.

c. Click **Add**.

6. Create a static route with IP address 192.168.50.0/24:

a. From the main menu, select Routing > Routing Table > Basic > Route Configuration. A screen similar to the following displays.

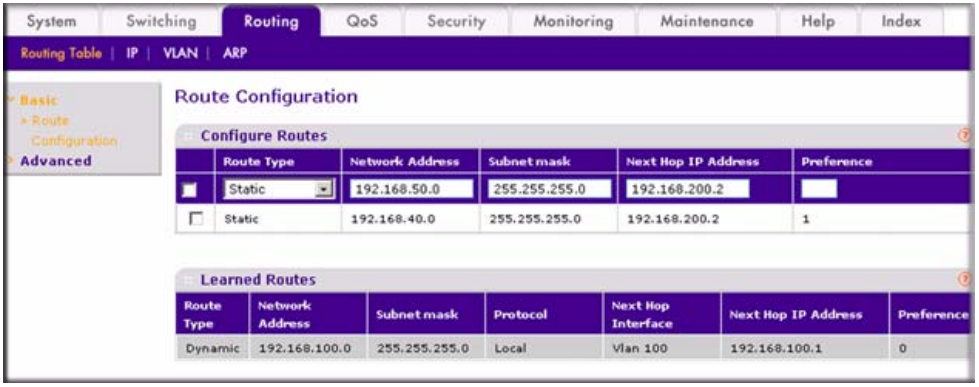


Figure 9-8

b. Under Configure Routes, make the following selection and enter the following information:

- Select **Static** from the Route Type pulldown menu.
- In the Network Address field, enter **192.168.50.0**.
- In the Subnet Mask field, enter **255.255.255.0**.
- In the Next Hop IP Address field, enter **192.168.200.2**.

c. Click **Add**.

7. Create an ACL with ID 101:

   a. From the main menu, select Security > ACL > Advanced > IP ACL. A screen similar to the following displays.

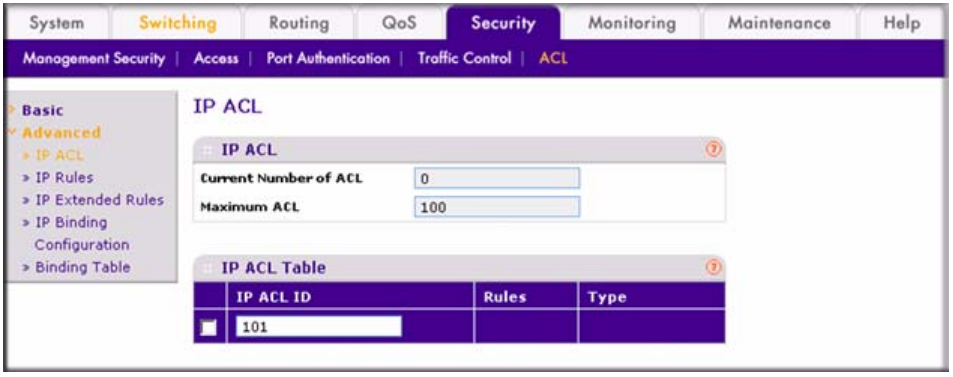


Figure 9-9

   b. In the IP ACL ID field of the IP ACL Table, enter **101**.

   c. Click **Add**.

8. Create an ACL with ID 102:

   a. From the main menu, select Security > ACL > Advanced > IP ACL. A screen similar to the following displays.

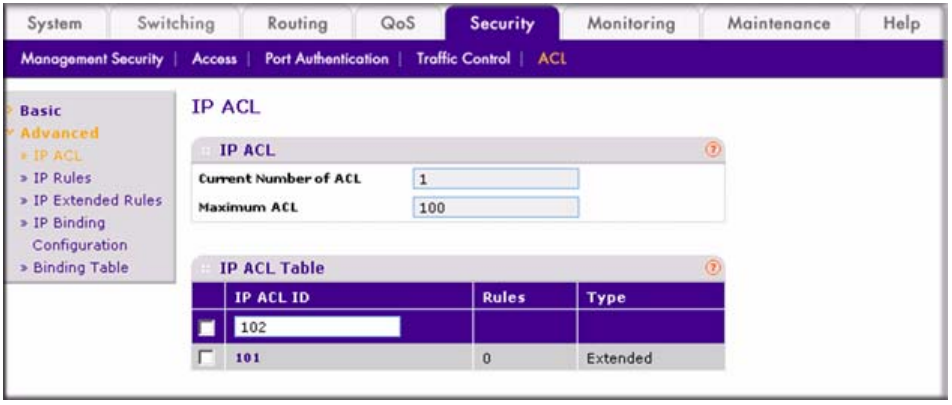


Figure 9-10

   b. In the IP ACL ID field of the IP ACL Table, enter **102**.

   c. Click **Add**.

9. Add and configure an IP extended rule that is associated with ACL 101:

a. From the main menu, select Security > ACL > Advanced > IP Extended Rules. A screen similar to the following displays.

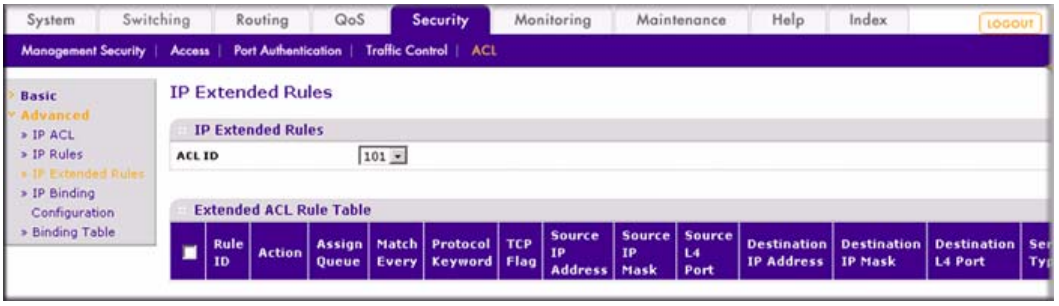


Figure 9-11

b. Under IP Extended Rules, select **101** from the ACL ID pulldown menu.

c. Click **Add**. The Extended ACL Rule Configuration screen displays.

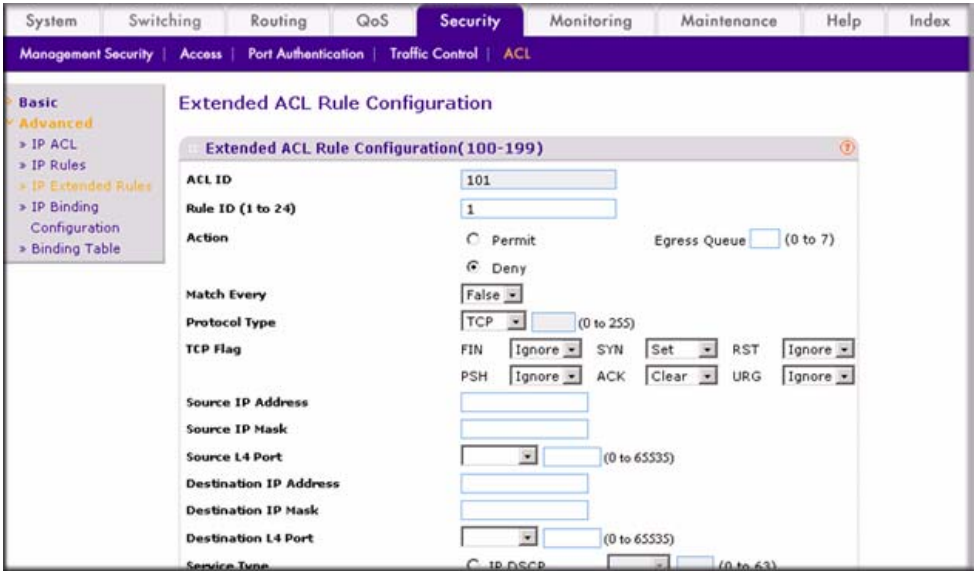


Figure 9-12

d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

- In the Rule ID field, enter **1**.
- Next to Action mode, select the **Deny** radio button.
- Select **False** from the Match Every pulldown menu.
- Select **TCP** from the Protocol Type pulldown menu.
- Next to TCP Flag, select **Set** from the SYN pulldown menu, and select **Clear** from the ACK pulldown menu.

e. Click **Apply** to save the settings.

10. Add and configure an IP extended rule that is associated with ACL 102:

a. From the main menu, select Security > ACL > Advanced > IP Extended Rules. A screen similar to the following displays.

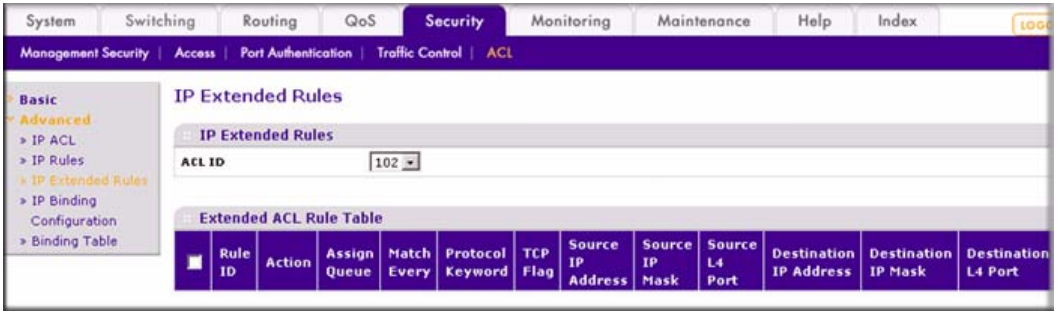


Figure 9-13

b. Under IP Extended Rules, select **102** from the ACL ID pulldown menu.

c. Click **Add**. The Extended ACL Rule Configuration screen displays.

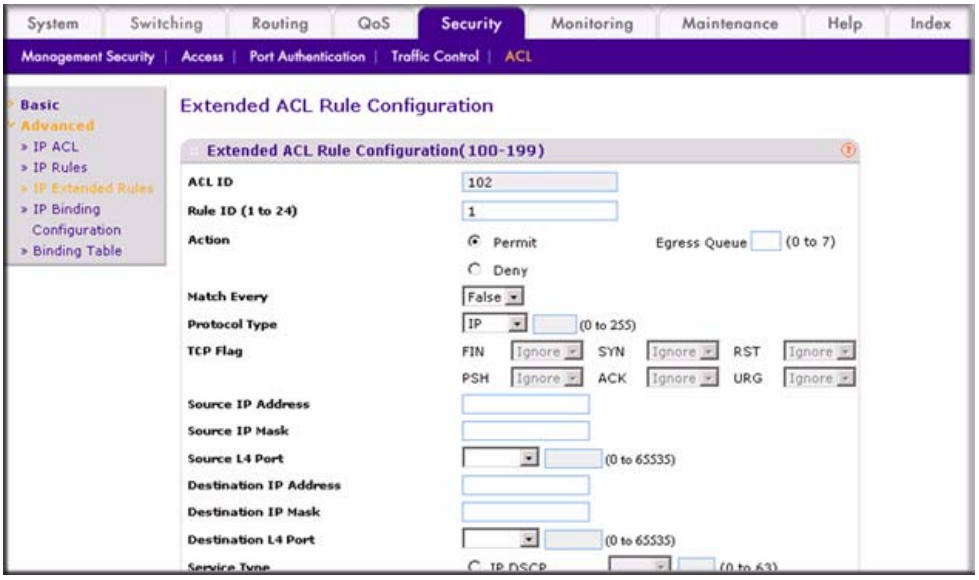


Figure 9-14

d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

- In the Rule ID field, enter **1**.
- Next to Action mode, select the **Permit** radio button.
- Select **False** from the Match Every pulldown menu.
- Select **IP** from the Protocol Type pulldown menu.

e. Click **Apply** to save the settings.

11. Apply ACL 101 to port 44:

a. From the main menu, select Security > ACL > Advanced > IP Binding Configuration. A screen similar to the following displays.

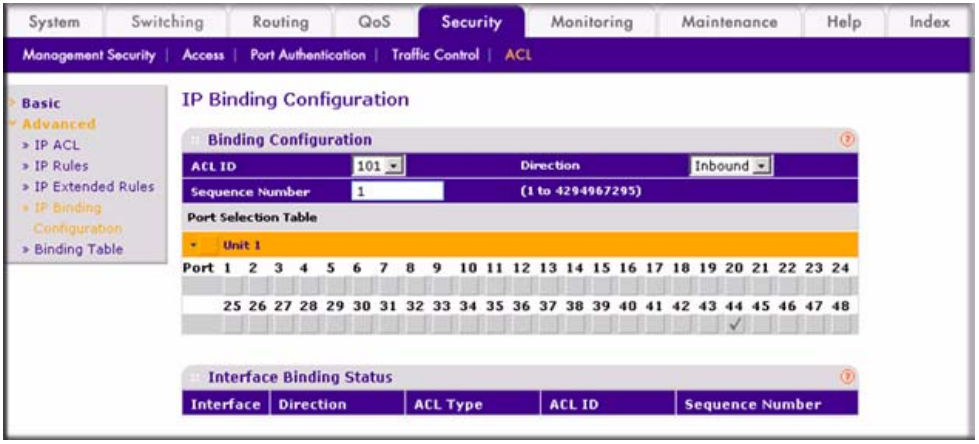


Figure 9-15

b. Under Binding Configuration, make the following selection and enter the following information:

- Select **101** from the ACL ID pulldown menu.
- In the Sequence Number field, enter **1**.

c. Click **Unit 1**. The ports display.

d. Click on the gray box under port 44. A flag appears in the box.

e. Click **Apply** to save the settings.

12. Apply ACL 102 to port 44:

a. From the main menu, select Security > ACL > Advanced > IP Binding Configuration. A screen similar to the following displays.

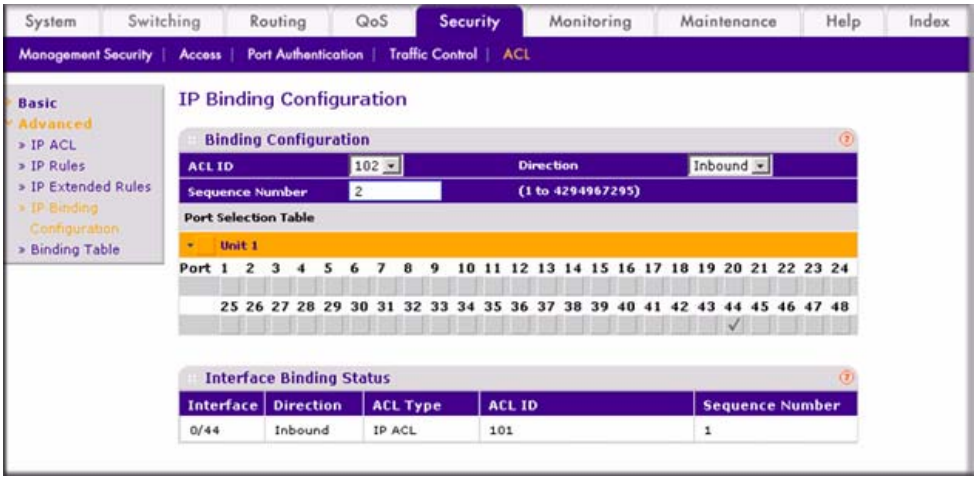


Figure 9-16

b. Under Binding Configuration, make the following selection and enter the following information:

- Select **102** from the ACL ID pulldown menu.
- In the Sequence Number field, enter **2**.

c. Click **Unit 1**. The ports display.

d. Click on the gray box under port 44. A flag appears in the box.

e. Click **Apply** to save the settings.

To use the Web interface to configure the GSM7352S, proceed as follows:

1. Create VLAN 40 with IP address 192.168.40.1/24:

a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.

System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Routing Table | IP | VLAN | ARP | RIP | OSPF | Router Discovery | VRRP
VLAN Routing Wizard
VLAN Routing
VLAN Routing Wizard
VLAN Routing Wizard
Vlan ID
40
LAG Enabled
IP Address
192.168.40.1
Network Mask
255.255.255.0
Unit 1
Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
U
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
49 50 51 52

Figure 9-17

b. Enter the following information in the VLAN Routing Wizard:

- In the Vlan ID field, enter **40**.
- In the IP Address field, enter **192.168.40.1**.
- In the Network Mask field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port 24 twice until **U** displays. The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 40.

2. Create VLAN 50 with IP address 192.168.50.1/24:

a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.

System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Routing Table | IP | VLAN | ARP | RIP | OSPF | Router Discovery | VRRP
VLAN Routing Wizard
VLAN Routing
VLAN Routing Wizard
VLAN Routing Wizard
Vlan ID
50
LAG Enabled
IP Address
192.168.50.1
Network Mask
255.255.255.0
Unit 1
Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
U
49 50 51 52

Figure 9-18

b. Enter the following information in the VLAN Routing Wizard:

- In the Vlan ID field, enter **50**.
- In the IP Address field, enter **192.168.50.1**.
- In the Network Mask field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port 25 twice until **U** displays. The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 50.

3. Create VLAN 200 with IP address 192.168.200.2/24:

a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.

System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Routing Table | IP | VLAN | ARP | RIP | OSPF | Router Discovery | VRRP
VLAN Routing Wizard
VLAN Routing
VLAN Routing Wizard
VLAN Routing Wizard
Vlan ID
200
LAG Enabled
IP Address
192.168.200.2
Network Mask
255.255.255.0
Unit 1
Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
U
49 50 51 52

Figure 9-19

b. Enter the following information in the VLAN Routing Wizard:

- In the Vlan ID field, enter **200**.
- In the IP Address field, enter **192.168.200.2**.
- In the Network Mask field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port 48 twice until **U** displays. The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 200.

4. Create a static route with IP address 192.168.100.0/24:

a. From the main menu, select Routing > Routing Table > Basic > Route Configuration. A screen similar to the following displays.

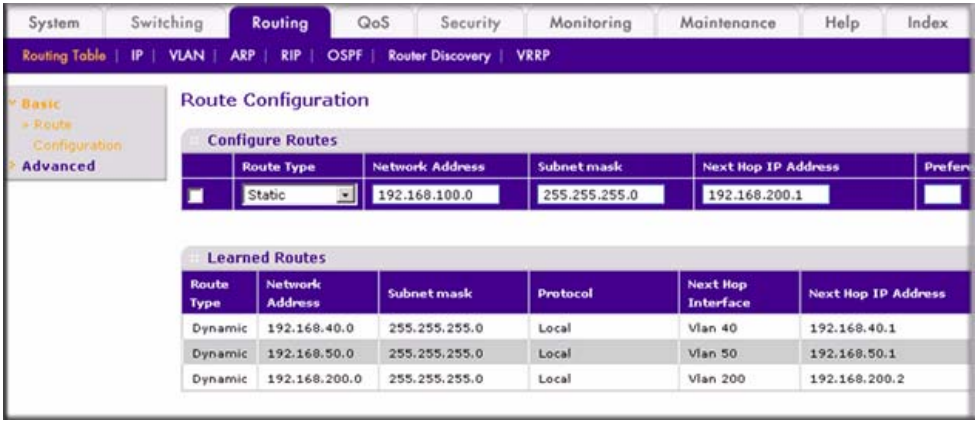


Figure 9-20

b. Under Configure Routes, make the following selection and enter the following information:

- Select **Static** from the Route Type pulldown menu.
- In the Network Address field, enter **192.168.100.0**.
- In the Subnet Mask field, enter **255.255.255.0**.
- In the Next Hop IP Address field, enter **192.168.200.1**.

c. Click **Add**.

5. Create a static route with IP address 192.168.30.0/24:

   a. From the main menu, select Routing > Routing Table > Basic > Route Configuration. A screen similar to the following displays.

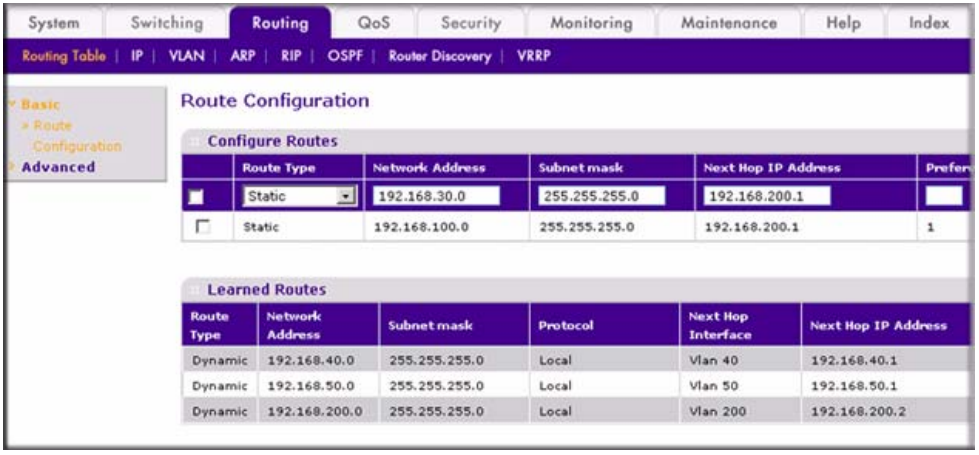


Figure 9-21

   b. Under Configure Routes, make the following selection and enter the following information:

      - Select **Static** from the Route Type pulldown menu.
      - In the Network Address field, enter **192.168.30.0**.
      - In the Subnet Mask field, enter **255.255.255.0**.
      - In the Next Hop IP Address field, enter **192.168.200.1**.

   c. Click **Add**.

Example #3: Configure Isolated VLANs on a Layer 3 switch by Using ACLs

This example shows how to isolate VLANs on a Layer 3 switch by using ACLs. In this example, PC1 is in VLAN 24, PC2 is in VLAN 48, and PC3 is in VLAN 38. PC1 and PC2 are isolated by an ACL but can both access the server.

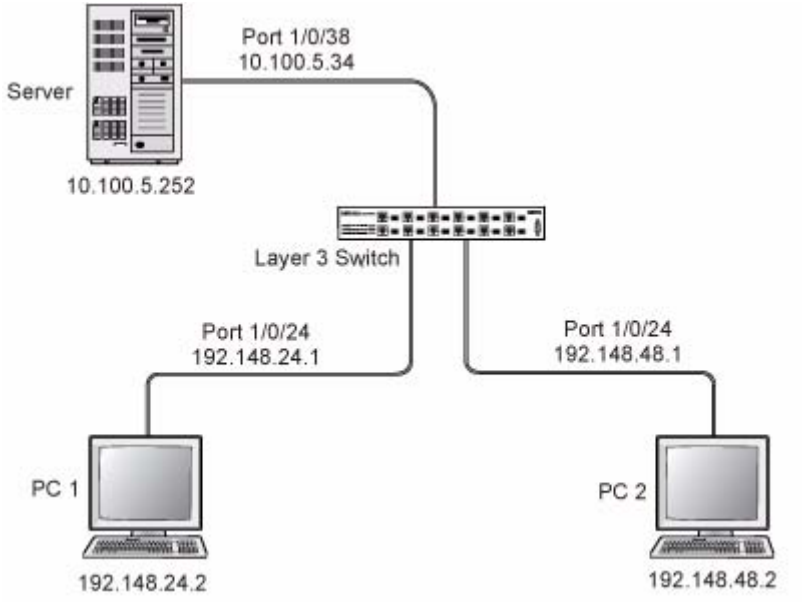


Figure 9-22

The example is shown as CLI commands and as a Web interface procedure.

CLI Commands

To use the CLI to isolate VLANs on a Layer 3 switch by using ACLs, enter the following CLI commands:

```
Create VLAN 24, add port 1/0/24 to it, and assign IP address 192.168.24.1 to it.
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 24
(Netgear Switch) (Vlan)#vlan routing 24
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan participation include 24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 24
(Netgear Switch) (Interface 1/0/24)#exit

(Netgear Switch) (Config)#interface vlan 24
(Netgear Switch) (Interface-vlan 24)#routing
(Netgear Switch) (Interface-vlan 24)#ip address 192.168.24.1 255.255.255.0
(Netgear Switch) (Interface-vlan 24)#exit
(Netgear Switch) (Config)#exit
```

```
Create VLAN 48, add port 1/0/48 to it, and assign IP address 192.168.48.1 to it.
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 48
(Netgear Switch) (Vlan)#vlan routing 48
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan participation include 48
(Netgear Switch) (Interface 1/0/48)#vlan pvid 48
(Netgear Switch) (Interface 1/0/48)#exit

(Netgear Switch) (Config)#vlan interface vlan 48
(Netgear Switch) (Interface-vlan 48)#routing
(Netgear Switch) (Interface-vlan 48)#ip address 192.168.48.1 255.255.255.0
(Netgear Switch) (Interface-vlan 48)#exit
(Netgear Switch) (Config)#exit

Create VLAN 38, add port 1/0/38 to it, and assign IP address 10.100.5.34 to it.
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 38
(Netgear Switch) (Vlan)#vlan routing
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/38
(Netgear Switch) (Interface 1/0/38)#vlan participation include 38
(Netgear Switch) (Interface 1/0/38)#vlan pvid 38
(Netgear Switch) (Interface 1/0/38)#exit

Netgear Switch) (Config)#interface vlan 38
(Netgear Switch) (Interface-vlan 38)#routing
(Netgear Switch) (Interface-vlan 38)#ip address 10.100.5.34 255.255.255.0
(Netgear Switch) (Interface-vlan 38)#exit

Enable IP routing on the switch.
(Netgear Switch) (Config)#ip routing

Add a default route so that all the traffic without a destination is forwarded
according to this default route.
(Netgear Switch) (Config)#ip route default 10.100.5.252

Create ACL 101 to deny all traffic that has destination IP 192.168.24.0/24.
(Netgear Switch) (Config)#access-list 101 deny ip any 192.168.24.0 0.0.0.255

Create ACL 102 to deny all traffic that has destination IP 192.168.48.0/24.
(Netgear Switch) (Config)#access-list 102 deny ip any 192.168.48.0 0.0.0.255
```

```
Create ACL 103 to permit all other traffic.
(Netgear Switch) (Config)#access-list 103 permit ip any any

Deny all traffic with destination IP address 192.168.48.0/24 and permit all
other traffic.
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#ip access-group 102 in 1
(Netgear Switch) (Interface 1/0/24)#ip access-group 103 in 2
(Netgear Switch) (Interface 1/0/24)#exit

Deny all traffic with destination IP address 192.168.24.0/24 and permit all
other traffic.
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#ip access-group 101 in 1
(Netgear Switch) (Interface 1/0/48)#ip access-group 103 in 2
(Netgear Switch) (Interface 1/0/48)#exit
```

Web Interface Procedure

To use the Web interface to isolate VLANs on a Layer 3 switch by using ACLs, proceed as follows:

1. Create VLAN 24 with IP address 192.168.24.1:
   a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.

System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Routing Table | IP | VLAN | ARP | RIP | OSPF | Router Discovery | VRRP
VLAN Routing Wizard
VLAN Routing
VLAN Routing Wizard
VLAN Routing Wizard
Vlan ID
24
LAG Enabled
IP Address
192.168.24.1
Network Mask
255.255.255.0
Unit 1
Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
49 50 51 52

Figure 9-23

b. Enter the following information in the VLAN Routing Wizard:

- In the Vlan ID field, enter **24**.
- In the IP Address field, enter **192.168.24.1**.
- In the Network Mask field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port 24 twice until **U** displays. The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 24.

2. Create VLAN 48 with IP address 192.168.48.1:

a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.

System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Routing Table | IP | VLAN | ARP | RIP | OSPF | Router Discovery | VRRP
VLAN Routing Wizard
VLAN Routing
VLAN Routing Wizard
VLAN Routing Wizard
Vlan ID
48
LAG Enabled
IP Address
192.168.48.1
Network Mask
255.255.255.0
Unit 1
Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
U
49 50 51 52

Figure 9-24

b. Enter the following information in the VLAN Routing Wizard:

- In the Vlan ID field, enter **48**.
- In the IP Address field, enter **192.168.48.1**.
- In the Network Mask field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port 48 twice until **U** displays. The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 48.

3. Create VLAN 38 with IP address 10.100.5.34:

a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.

System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Routing Table | IP | VLAN | ARP | RIP | OSPF | Router Discovery | VRRP
VLAN Routing Wizard
VLAN Routing
VLAN Routing Wizard
VLAN Routing Wizard
Vlan ID
38
LAG Enabled
IP Address
10.100.5.34
Network Mask
255.255.255.0
Unit 1
Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
U
49 50 51 52

Figure 9-25

b. Enter the following information in the VLAN Routing Wizard:

- In the Vlan ID field, enter **38**.
- In the IP Address field, enter **10.100.5.34**.
- In the Network Mask field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port 38 twice until **U** displays. The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 38.

4. Enable IP Routing:

a. From the main menu, select Routing > IP > Basic > IP Configuration. A screen similar to the following displays.

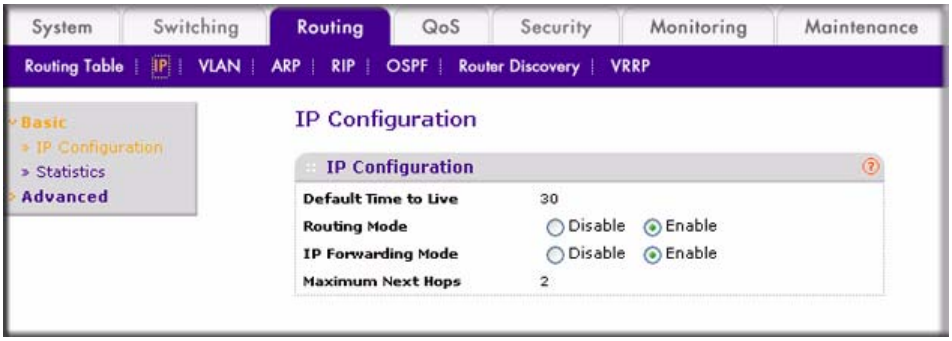


Figure 9-26

b. Under IP Configuration, make the following selections:

- Next to Routing Mode, select the **Enable** radio button.
- Next to IP Forwarding Mode, select the **Enable** radio button.

c. Click **Apply** to enable IP Routing.

5. Create an ACL with ID 101:

a. From the main menu, select Security > ACL > Advanced > IP ACL. A screen similar to the following displays.

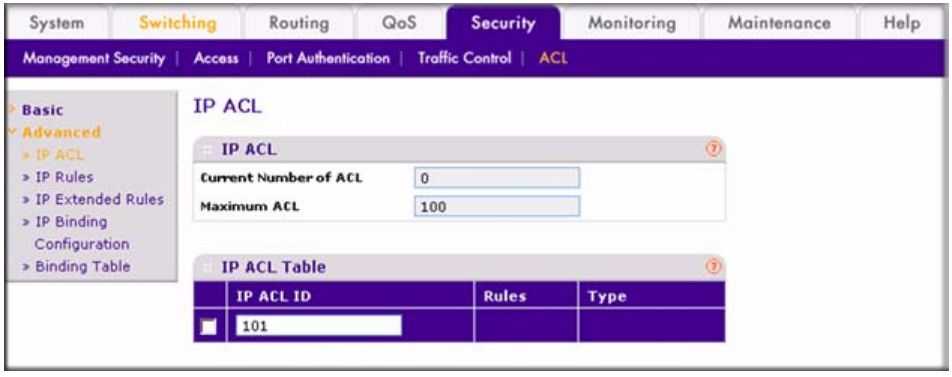


Figure 9-27

b. In the IP ACL ID field of the IP ACL Table, enter **101**.

c. Click **Add**.

6. Create an ACL with ID 102:

   a. From the main menu, select Security > ACL > Advanced > IP ACL. A screen similar to the following displays.

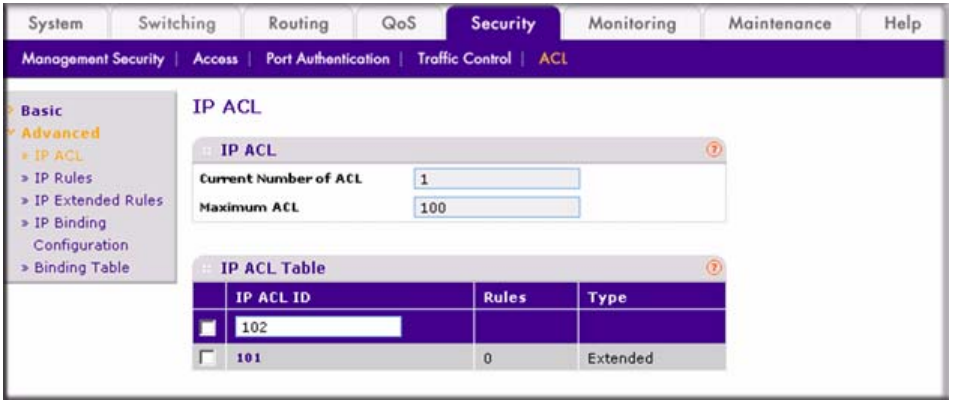


Figure 9-28

   b. In the IP ACL ID field of the IP ACL Table, enter **102**.

   c. Click **Add**.

7. Create an ACL with ID 103:

   a. From the main menu, select Security > ACL > Advanced > IP ACL. A screen similar to the following displays.

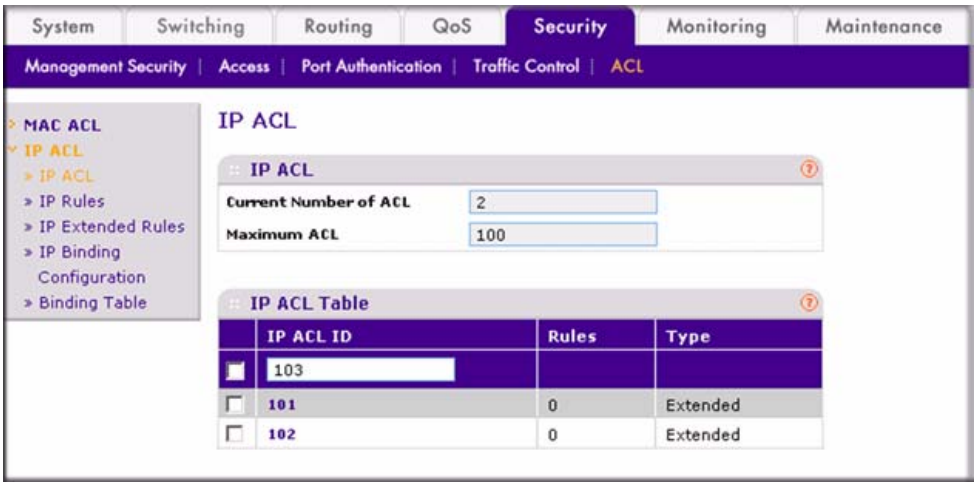


Figure 9-29

b. In the IP ACL ID field of the IP ACL Table, enter **103**.

c. Click **Add**.

8. Add and configure an IP extended rule that is associated with ACL 101:

a. From the main menu, select Security > ACL > Advanced > IP Extended Rules. A screen similar to the following displays.

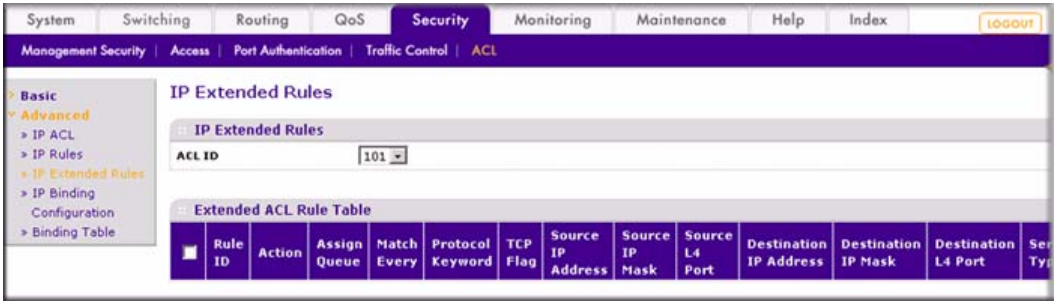


Figure 9-30

b. Under IP Extended Rules, select **101** from the ACL ID pulldown menu.

c. Click **Add**. The Extended ACL Rule Configuration screen displays.

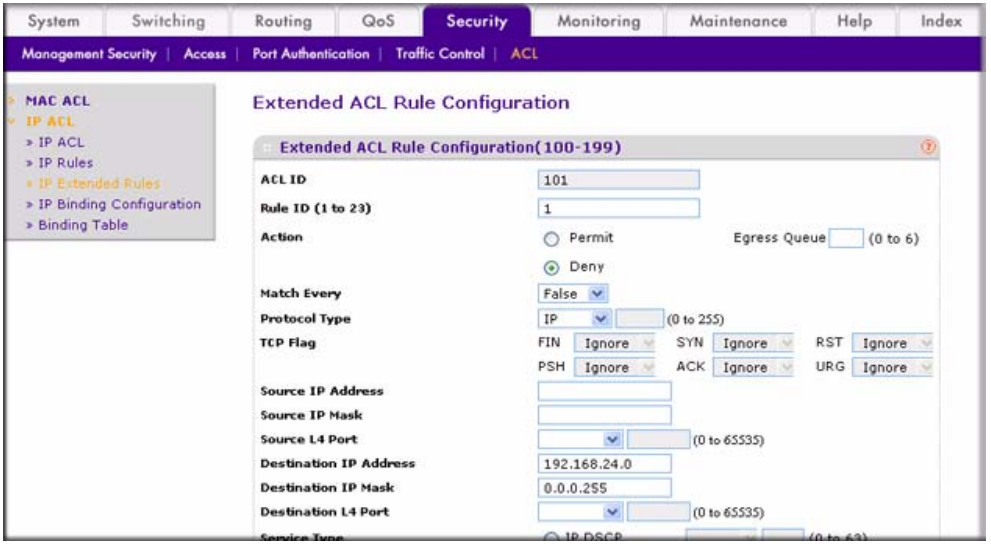


Figure 9-31

d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

- In the Rule ID field, enter **1**.
- Next to Action mode, select the **Deny** radio button.
- Select **False** from the Match Every pulldown menu.
- In the Destination IP Address field, enter **192.168.24.0**.
- In the Destination IP Mask field, enter **0.0.0.255**.

e. Click **Apply** to save the settings.

9. Add and configure an IP extended rule that is associated with ACL 102:

a. From the main menu, select Security > ACL > Advanced > IP Extended Rules. A screen similar to the following displays.

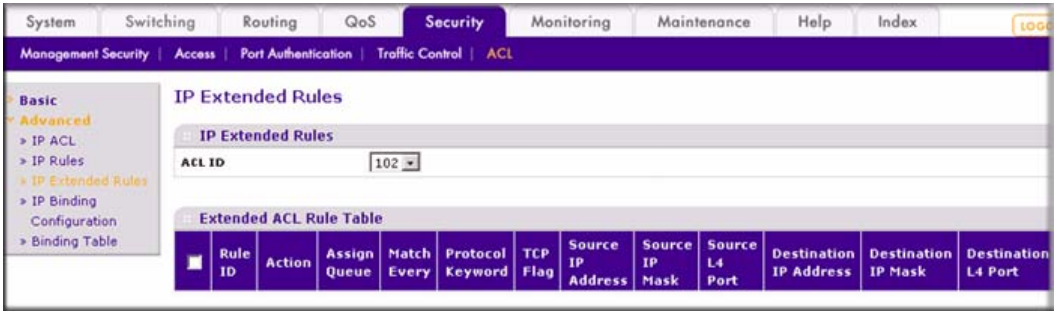


Figure 9-32

b. Under IP Extended Rules, select **102** from the ACL ID pulldown menu.

c. Click **Add**. The Extended ACL Rule Configuration screen displays.

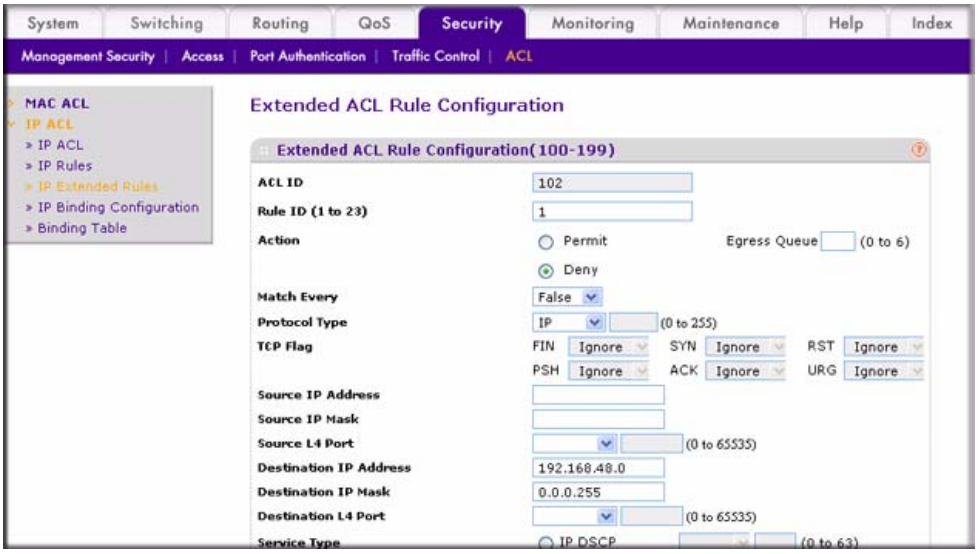


Figure 9-33

d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

- In the Rule ID field, enter **1**.
- Next to Action mode, select the **Deny** radio button.
- Select **False** from the Match Every pulldown menu.
- In the Destination IP Address field, enter **192.168.48.0**.
- In the Destination IP Mask field, enter **0.0.0.255**.

e. Click **Apply** to save the settings.

10. Add and configure an IP extended rule that is associated with ACL 103:

a. From the main menu, select Security > ACL > Advanced > IP Extended Rules. A screen similar to the following displays.

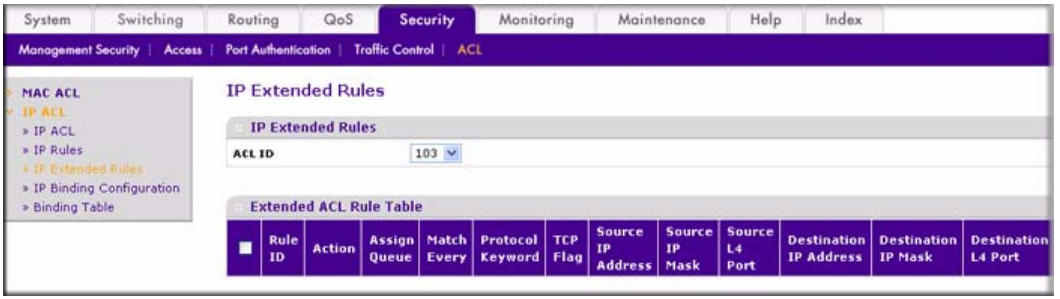


Figure 9-34

b. Under IP Extended Rules, select **103** from the ACL ID pulldown menu.

c. Click **Add**. The Extended ACL Rule Configuration screen displays.

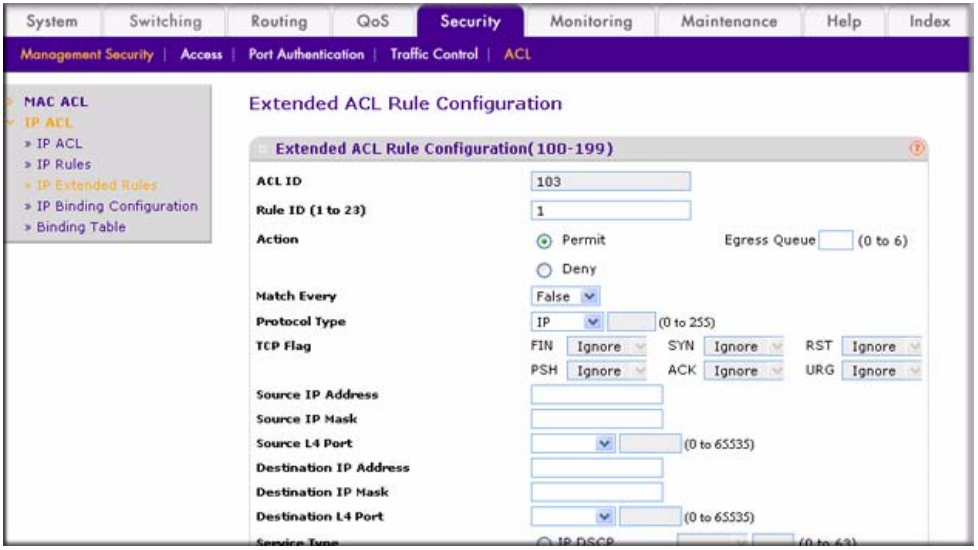


Figure 9-35

d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

- In the Rule ID field, enter **1**.

- Next to Action mode, select the **Permit** radio button.
- Select **False** from the Match Every pulldown menu.
- Select **IP** from the Protocol Type pulldown menu.

e. Click **Apply** to save the settings.

11. Apply ACL 102 to port 24:

a. From the main menu, select Security > ACL > Advanced > IP Binding Configuration. A screen similar to the following displays.

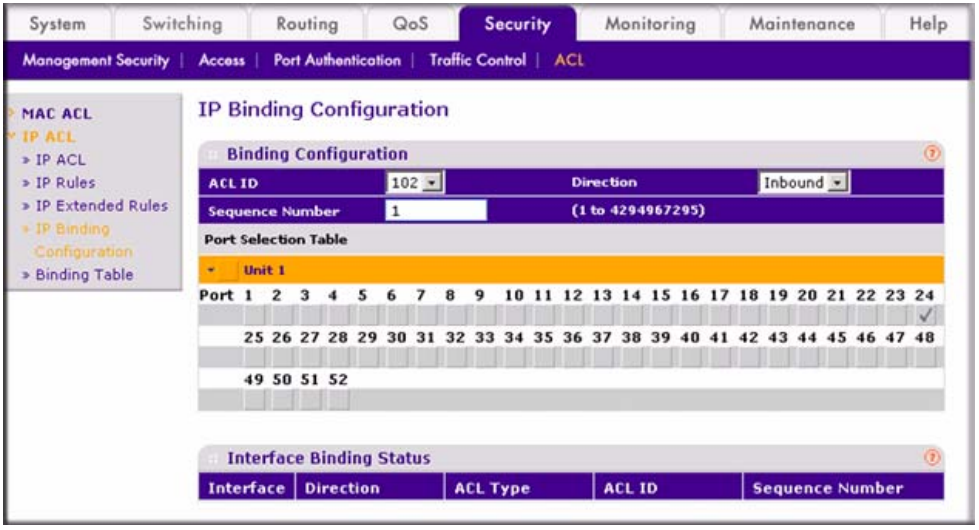


Figure 9-36

b. Under Binding Configuration, make the following selection and enter the following information:

- Select **102** from the ACL ID pulldown menu.
- In the Sequence Number field, enter **1**.

c. Click **Unit 1**. The ports display.

d. Click on the gray box under port 24. A flag appears in the box.

e. Click **Apply** to save the settings.

12. Apply ACL 101 to port 48:

a. From the main menu, select Security > ACL > Advanced > IP Binding Configuration. A screen similar to the following displays.

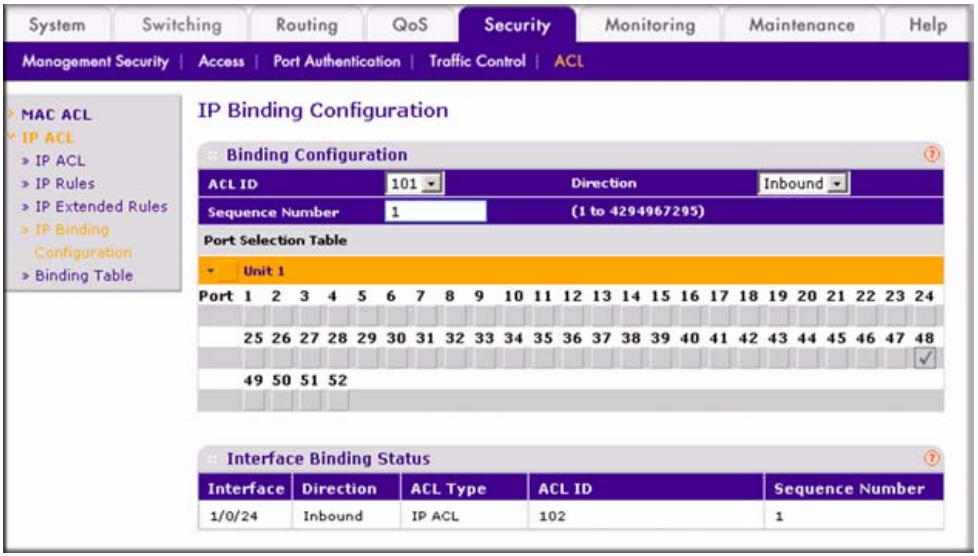


Figure 9-37

b. Under Binding Configuration, make the following selection and enter the following information:

- Select **101** from the ACL ID pulldown menu.
- In the Sequence Number field, enter **1**.

c. Click **Unit 1**. The ports display.

d. Click on the gray box under port 48. A flag appears in the box.

e. Click **Apply** to save the settings.

13. Apply ACL 103 to port 24 and port 48:

a. From the main menu, select Security > ACL > Advanced > IP Binding Configuration. A screen similar to the following displays.

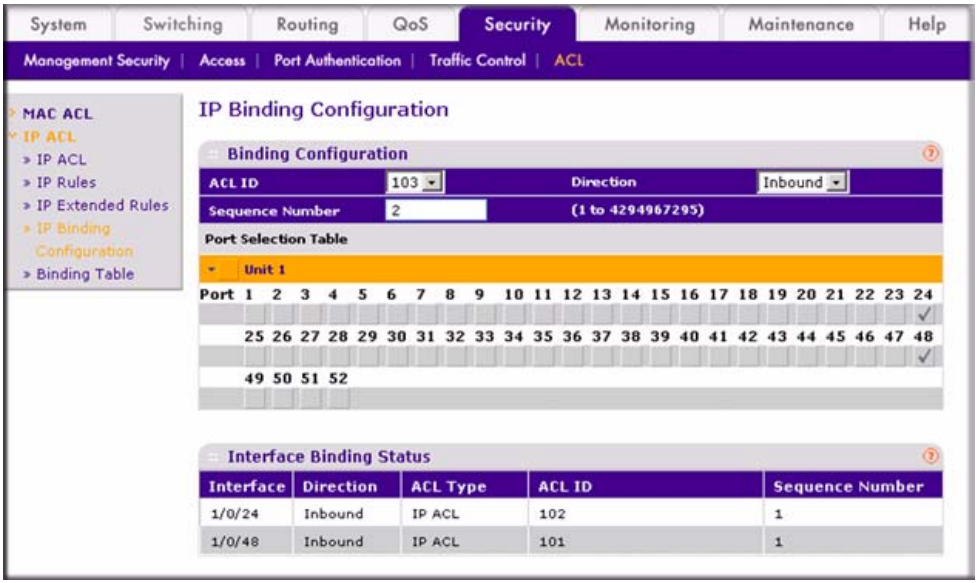

System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Management Security | Access | Port Authentication | Traffic Control | ACL
MAC ACL
IP ACL
» IP ACL
» IP Rules
» IP Extended Rules
» IP Binding Configuration
» Binding Table
IP Binding Configuration
Binding Configuration
ACL ID 103 Direction Inbound
Sequence Number 2 (1 to 4294967295)
Port Selection Table
Unit 1
Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
49 50 51 52
Interface Binding Status
Interface Direction ACL Type ACL ID Sequence Number
1/0/24 Inbound IP ACL 102 1
1/0/48 Inbound IP ACL 101 1

Figure 9-38

b. Under Binding Configuration, make the following selection and enter the following information:

- Select **103** from the ACL ID pulldown menu.
- In the Sequence Number field, enter **2**.

c. Click **Unit 1**. The ports display. Configure the following ports:

- Click on the gray box under port 24. A flag appears in the box.
- Click on the gray box under port 48. A flag appears in the box.

d. Click **Apply** to save the settings.

MAC ACL CLI Examples

The following are examples of the commands used for the MAC ACLs feature.

Example #1: mac access list

```
(Netgear Switch)(Config)#mac access-list ?

extended     Configure extended MAC Access List parameters.

Netgear Switch)(Config)#mac access-list extended ?

<name>    Enter access-list name up to 31 characters in length.
rename    Rename MAC Access Control List.

(Netgear Switch) (Config)#mac access-list extended b1 ?

<cr>      Press Enter to execute the command.

(Netgear Switch) (Config)#mac access-list extended b1
```

Example #2: permit any

```
(Netgear Switch) (Config-mac access-list)#permit ?

<srcmac>    Enter a MAC address.
any         Configure a match condition for all the destination MAC
            addresses in the Destination MAC Address field.

(Netgear Switch) (Config-mac access-list)#permit any ?

<dstmac>    Enter a MAC address.
any         Configure a match condition for all the destination MAC
            addresses in the Destination MAC Address field.


(Netgear Switch) (Config-mac access-list)#permit any any ?

assign-queue     Configure the Queue Id assignment attribute.
cos              Configure a match condition based on a CoS value.
<ethertypekey>   Enter one of the following keywords to specify an Ethertype
                (appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast,
                 netbios, novell, pppo, rarp).
<0x0600-0xffff)  Enter a four-digit hexadecimal number in the range of 0x0600 to
                 0xffff to specify a custom Ethertype value.
vlan             Configure a match condition based on a VLAN ID.
<cr>             Press Enter to execute the command.

(Netgear Switch) (Config-mac access-list)#permit any any
```

Example #3 Configure mac access-group

```
(Netgear Switch) (Config)#interface 1/0/5

(Netgear Switch) (Interface 1/0/5)#mac ?

access-group    Attach MAC Access List to Interface.

(Netgear Switch) (Interface 1/0/5)#mac access-group ?

<name>    Enter name of MAC Access Control List.

(Netgear Switch) (Interface 1/0/5)#mac access-group b1 ?

in    Enter the direction <in>.

(Netgear Switch) (Interface 1/0/5)#mac access-group b1 in ?

<cr>              Press Enter to execute the command.

<1-4294967295>    Enter the sequence number (greater than 0) to rank precedence
                  for this interface and direction. A lower sequence number has
                  higher precedence.

(Netgear Switch) (Interface 1/0/5)#mac access-group b1 in
```

Example #4 permit

```
(Netgear Switch) (Config)#mac access-list extended b2

(Netgear Switch) (Config-mac-access-list)#permit 00:00:00:00:00:00 ?

<dstmac>        Enter a MAC Address.
any             Configure a a match condition for all the destination MAC
                addresses in the Destination MAC Address field.

(Netgear Switch) (Config-mac-access-list)#permit 00:00:00:00:00:00 any

access-queue    Configure the Queue Id assignment attribute.
cos             Configure a match condition based on a CoS value.
<ethertypekey>  Enter one of the following keywords to specify an Ethertype
               (appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast,
                netbios, novell, pppo,rarp).
<0x0600-0xffff) Enter a four-digit hexadecimal number in the range of 0x0600 to
                0xffff to specify a custom Ethertype value.
vlan            Configure a match condition based on a VLAN ID.
<cr>            Press Enter to execute the command.
```

Example #5: show mac access-lists

```
(Netgear Switch) #show mac access-lists
Current number of all ACLs: 2    Maximum number of all ACLs: 100

MAC ACL Name    Rules     Interface(s)     Direction
------------    -----    ------------    ---------
b1              1        1/0/5           inbound
b2              1

(Netgear Switch)     #show mac access-lists ?

<name>    Enter access-list name up to 31 characters in length.
<cr>      Press Enter to execute the command.

(Netgear Switch)     #show mac access-lists b1 ?

<cr>      Press Enter to execute the command.

(Netgear Switch)     #show mac access-lists b1

Rule Number: 1
Action.................................    permit
Match All..............................    TRUE
```

Chapter 10
Class of Service (CoS) Queuing

This section describes the Class of Service (CoS) Queue Mapping and Traffic Shaping features.

Overview

Each port has one or more queues for packet transmission. During configuration, you can determine the mapping and configuration of these queues.

Based on service rate and other criteria you configure, queues provide preference to specified packets. If a delay becomes necessary, the system holds packets until the scheduler authorizes transmission. As queues become full, packets are dropped. Packet drop precedence indicates the packet's sensitivity to being dropped during times of queue congestion.

CoS mapping, queue parameters, and queue management are configurable per interface.

Queue management is configurable per interface.

Some hardware implementations allow queue depth management using tail dropping or Weighted random early discard (WRED).

Some hardware implementations allow queue depth management using tail dropping.

The operation of CoS Queuing involves queue mapping and queue configuration.

CoS Queue Mapping

CoS Queue Mapping uses trusted and untrusted ports.

Trusted Ports

- System takes at face value certain priority designation for arriving packets.
- Trust applies only to packets that have that trust information.
- Can only have one trust field at a time - per port.
  - 802.1p User Priority (default trust mode - Managed through Switching configuration)

  - IP Precedence
  - IP DiffServ Code Point (DSCP)

The system can assign service level based upon the 802.1p priority field of the L2 header. You configure this by mapping the 802.1p priorities to one of three traffic class queues. These queues are:

- Queue 2 - Minimum of 50% of available bandwidth
- Queue 1 - Minimum of 33% of available bandwidth
- Queue 0 - Lowest priority, minimum of 17% of available bandwidth

For untagged traffic, you can specify default 802.1p priority on a per-port basis.

Untrusted Ports

- No incoming packet priority designation is trusted, therefore the port default priority value is used.
- All ingress packets from Untrusted ports, where the packet is classified by an ACL or a DiffServ policy, are directed to specific CoS queues on the appropriate egress port. That specific CoS queue is determined by either the default priority of the port or a DiffServ or ACL assign queue attribute.
- Used when trusted port mapping is unable to be honored - i.e. when a non-IP DSCP packet arrives at a port configured to trust IP DSCP.

CoS Queue Configuration

CoS queue configuration involves port egress queue configuration and drop precedence configuration (per queue). The design of these on a per queue, per drop precedence basis allows the user to create the desired service characteristics for different types of traffic.

Port Egress Queue Configuration

- Scheduler Type
  - Strict vs. Weighted
- Minimum guaranteed bandwidth
- Maximum allowed bandwidth
  - Per queue shaping
- Queue management type

  - Tail drop vs. WRED

Drop Precedence Configuration (per Queue)

- WRED parameters
  - Minimum threshold
  - Maximum threshold
  - Drop probability
  - Scale factor
- Tail Drop parameters
  - Threshold

Per-Interface Basis

- Queue management type
  - Tail Drop vs. WRED

Only if per queue config is not supported

- WRED Decay Exponent
- Traffic Shaping
  - For an entire interface

CLI Examples

The following are examples of the commands used in the CoS Queuing feature.

Example #1: show classofservice trust

```
(Netgear Switch) #show classofservice trust ?

<cr>                    Press Enter to execute the command.

(Netgear Switch) #show classofservice trust

Class of Service Trust Mode: Dot1P
```

Example #2: set classofservice trust mode

```
(Netgear Switch) (Config)#classofservice ?

dot1p-mapping            Configure dot1p priority mapping.
ip-dscp-mapping          Maps an IP DSCP value to an internal traffic class.
trust                    Sets the Class of Service Trust Mode of an Interface.

(Netgear Switch) (Config)#classofservice trust ?

dot1p                    Sets the Class of Service Trust Mode of an Interface
                         to 802.1p.
ip-dscp                  Sets the Class of Service Trust Mode of an Interface
                         to IP DSCP.

(Netgear Switch) (Config)#classofservice trust dot1p ?

<cr>                     Press Enter to execute the command.

(Netgear Switch) (Config)#classofservice trust dot1p
```

Example #3: show classofservice ip-precedence mapping

```
(Netgear Switch) #show classofservice ip-precedence-mapping

IP Precedence    Traffic Class
-------------    -------------
    0                1
    1                0
    2                0
    3                1
    4                2
    5                2
    6                3
    7                3
```

Example #4: Config Cos-queue Min-bandwidth and Strict Priority Scheduler Mode

```
(Netgear Switch) (Config)#cos-queue min-bandwidth ?

<bw-0>                   Enter the minimum bandwidth percentage for Queue 0.

(Netgear Switch) (Config)#cos-queue min-bandwidth 15

Incorrect input! Use 'cos-queue min-bandwidth <bw-0>..<bw-7>.

(Netgear Switch) (Config)#cos-queue min-bandwidth 15 25 10 5 5 20 10 10


(Netgear Switch) (Config)#cos-queue strict ?

<queue-id>               Enter a Queue Id from 0 to 7.

(Netgear Switch) (Config)#cos-queue strict 1 ?

<cr>                     Press Enter to execute the command.
<queue-id>               Enter an additional Queue Id from 0 to 7.

(Netgear Switch) (Config)#cos-queue strict 1
```

Example #5: Set CoS Trust Mode of an Interface

```
(Netgear Switch) (Config)#classofservice trust ?

dot1p                    Sets the Class of Service Trust Mode of an Interface
                         to 802.1p.
ip-dscp                  Sets the Class of Service Trust Mode of an Interface
                         to IP DSCP.

(Netgear Switch) (Config)#classofservice trust dot1p ?

<cr>                     Press Enter to execute the command.

(Netgear Switch) (Config)#classofservice trust dot1p
```

Note: The Traffic Class value range is <0-6> instead of <0-7> because queue 7 is reserved in a stacking build for stack control, and is therefore not configurable by the user.

Traffic Shaping

This section describes the Traffic Shaping feature.

Traffic shaping controls the amount and volume of traffic transmitted through a network. This has the effect of smoothing temporary traffic bursts over time.

CLI Example

Use the *traffic-shape* command to enable traffic shaping by specifying the maximum transmission bandwidth limit for all interfaces (Global Config) or for a single interface (Interface Config).

The <bw> value is a percentage that ranges from 0 to 100 in increments of 5. The default bandwidth value is 0, meaning no upper limit is enforced, which allows the interface to transmit up to its maximum line rate.

The bw value is independent of any per-queue maximum bandwidth value(s) in effect for the interface and should be considered as a second-level transmission rate control mechanism that regulates the output of the entire interface regardless of which queues originate the outbound traffic.

Example #1 traffic-shape

```
(Netgear Switch) (Config)#traffic-shape ?

<bw>                    Enter the shaping bandwidth percentage from 0 to 100
                        in increments of 5.

(Netgear Switch) (Config)#traffic-shape 70 ?

<cr>                    Press Enter to execute the command.

(Netgear Switch) (Config)#traffic-shape 70

(Netgear Switch) (Config)#
```

Chapter 11
Differentiated Services

Differentiated Services (DiffServ) is one technique for implementing Quality of Service (QoS) policies. Using DiffServ in your network allows you to directly configure the relevant parameters on the switches and routers rather than using a resource reservation protocol.This section explains how to configure the 7000 Series Managed Switch to identify which traffic class a packet belongs to, and how it should be handled to provide the desired quality of service. As implemented on the 7000 Series Managed Switch, DiffServ allows you to control what traffic is accepted and what traffic is discarded.

How you configure DiffServ support on a 7000 Series Managed Switch varies depending on the role of the switch in your network:

- **Edge device.** An edge device handles ingress traffic, flowing towards the core of the network, and egress traffic, flowing away from the core. An edge device segregates inbound traffic into a small set of traffic classes, and is responsible for determining a packet's classification. Classification is primarily based on the contents of the Layer 3 and Layer 4 headers, and is recorded in the Differentiated Services Code Point (DSCP) added to a packet's IP header.
- **Interior node.** A switch in the core of the network is responsible for forwarding packets, rather than for classifying them. It decodes the DSCP code point in an incoming packet, and provides buffering and forwarding services using the appropriate queue management algorithms.

Before configuring DiffServ on a particular 7000 Series Managed Switch, you must determine the QoS requirements for the network as a whole. The requirements are expressed in terms of rules, which are used to classify inbound traffic on a particular interface. The switch software does not support DiffServ in the outbound direction.

Rules are defined in terms of classes, policies and services:

- **Class.** A class consists of a set of rules that identify which packets belong to the class. Inbound traffic is separated into traffic classes based on Layer 3 and 4 header data and the VLAN ID, and marked with a corresponding DSCP value. One type of class is supported: **All,** which specifies that every match criterion defined for the class must be true for a match to occur.
- **Policy.** Defines the QoS attributes for one or more traffic classes. An example of an attribute is the ability to mark a packet at ingress. The 7000 Series Managed Switch supports a Traffic Conditions Policy. This type of policy is associated with an inbound traffic class and specifies the actions to be performed on packets meeting the class rules:

  - Marking the packet with a given DSCP code point, IP precedence, or CoS
  - Policing packets by dropping or re-marking those that exceed the class's assigned data rate
  - Counting the traffic within the class
- **Service.** Assigns a policy to an interface for inbound traffic

CLI Example

This example shows how a network administrator can provide equal access to the Internet (or other external network) to different departments within a company. Each of four departments has its own Class B subnet that is allocated 25% of the available bandwidth on the port accessing the Internet.

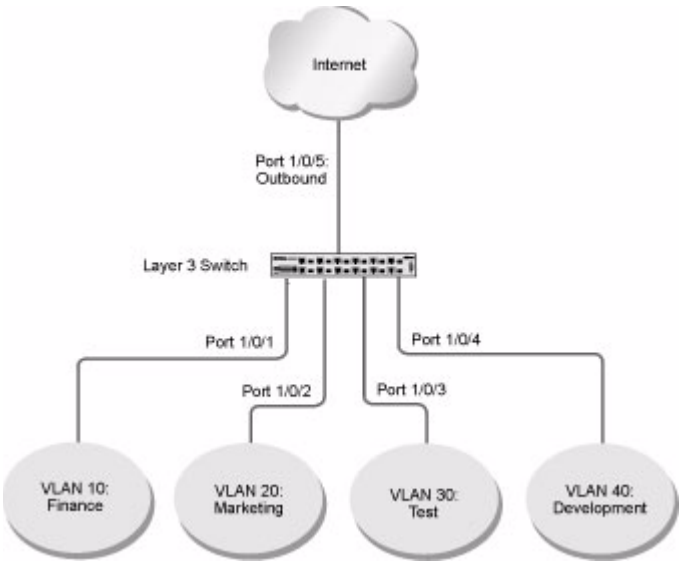


Figure 11-1

The following example configures DiffServ on a 7000 Series Managed Switch:

```
            Ensure DiffServ operation is enabled for the switch.
(Netgear Switch) #config
(Netgear Switch) (Config)#diffserv


            Create a DiffServ class of type “all” for each of the departments,
            and name them. Define the match criteria -- Source IP address --
            for the new classes.

(Netgear Switch) (Config)#class-map match-all finance_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.10.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit

(Netgear Switch) (Config)#class-map match-all marketing_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.20.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit

(Netgear Switch) (Config)#class-map match-all test_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.30.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit

(Netgear Switch) (Config)#class-map match-all development_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.40.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit


            Create a DiffServ policy for inbound traffic named
            'internet_access', adding the previously created department
            classes as instances within this policy.
            This policy uses the assign-queue attribute to put each depart-
            ment's traffic on a different egress queue.  This is how the Diff-
            Serv inbound policy connects to the CoS queue settings established
            below.

(Netgear Switch) (Config)#policy-map internet_access in
(Netgear Switch) (Config policy-map)#class finance_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 1
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class marketing_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 2
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class test_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 3
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class development_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 4
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#exit
```

```
              Attach the defined policy to interfaces 1/0/1 through 1/0/4 in the
              inbound direction

(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/1)#exit

(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/2)#exit

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/3)#exit

(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/4)#exit

              Set the CoS queue configuration for the (presumed) egress inter-
              face 1/0/5 such that each of queues 1, 2, 3 and 4 get a minimum
              guaranteed bandwidth of 25%.  All queues for this interface use
              weighted round robin scheduling
              by default. The DiffServ inbound policy designates that these
              queues are to be used for the departmental traffic through the
              assign-queue attribute.  It is presumed that the switch will for-
              ward this traffic to interface 1/0/5 based on a normal destination
              address lookup for internet traffic.

(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#cos-queue min-bandwidth 0 25 25 25 25 0 0 0
(Netgear Switch) (Interface 1/0/5)#exit
(Netgear Switch) (Config)#exit
```

DiffServ for VoIP Configuration Example

One of the most valuable uses of DiffServ is to support Voice over IP (VoIP). VoIP traffic is inherently time-sensitive: for a network to provide acceptable service, a guaranteed transmission rate is vital. This example shows one way to provide the necessary quality of service: how to set up

a class for UDP traffic, have that traffic marked on the inbound side, and then expedite the traffic on the outbound side. The configuration script is for Router 1 in the accompanying diagram: a similar script should be applied to Router 2.

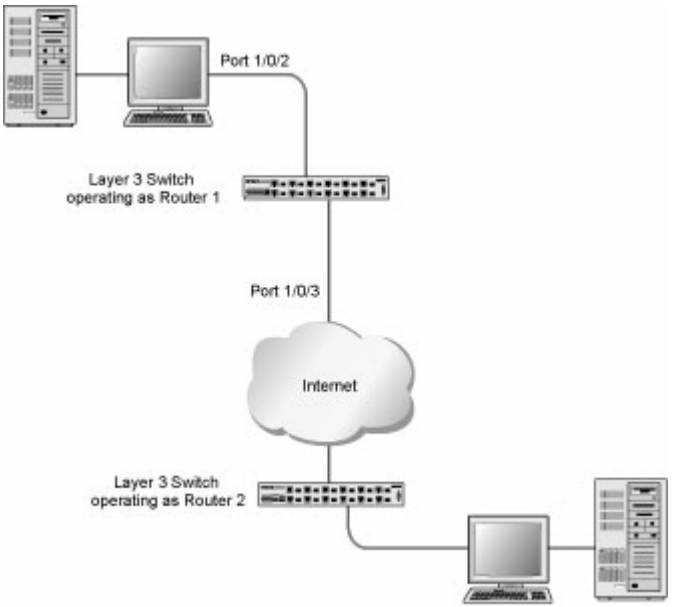


Figure 11-2

The following example configures DiffServ VoIP support:

```
            Enter Global Config mode. Set queue 5 on all ports to use strict
            priority mode.  This queue shall be used for all VoIP packets.
            Activate DiffServ for the switch.
(Netgear Switch) #config
(Netgear Switch) (Config)#cos-queue strict 5
(Netgear Switch) (Config)#diffserv

            Create a DiffServ classifier named 'class_voip' and define a sin-
            gle match criterion to detect UDP packets. The class type "match-
            all" indicates that all match criteria defined for the class must
            be satisfied in order for a packet to be considered a match.

(Netgear Switch) (Config)#class-map match-all class_voip
(Netgear Switch) (Config class-map)#match protocol udp
(Netgear Switch) (Config class-map)#exit

            Create a second DiffServ classifier named 'class_ef' and define a
            single match criterion to detect a DiffServ code point (DSCP) of
            'EF' (expedited forwarding). This handles incoming traffic that
            was previously marked as expedited somewhere in the network.

(Netgear Switch) (Config)#class-map match-all class_ef
(Netgear Switch) (Config class-map)#match ip dscp ef
(Netgear Switch) (Config class-map)#exit
            Create a DiffServ policy for inbound traffic named 'pol_voip',
            then add the previously created classes 'class_ef' and
            'class_voip' as instances within this policy.
            This policy handles incoming packets already marked with a DSCP
            value of 'EF' (per 'class_ef' definition), or marks UDP packets
            per the 'class_voip' definition) with a DSCP value of 'EF'. In
            each case, the matching packets are assigned internally to use
            queue 5 of the egress port to which they are forwarded.

(Netgear Switch) (Config)#policy-map pol_voip in
(Netgear Switch) (Config policy-map)#class class_ef
(Netgear Switch) (Config policy-class-map)#assign-queue 5
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class class_voip
(Netgear Switch) (Config policy-class-map)#mark ip-dscp ef
(Netgear Switch) (Config policy-class-map)#assign-queue 5
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#exit

            Attach the defined policy to an inbound service interface.

(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#service-policy in pol_voip
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Chapter 12
IGMP Snooping

This section describes the Internet Group Management Protocol (IGMP) feature: IGMPv3 and IGMP Snooping.

Overview

IGMP:

- Uses Version 3 of IGMP
- Includes snooping
- Snooping can be enabled per VLAN

CLI Examples

The following are examples of the commands used in the IGMP Snooping feature.

Example #1: Enable IGMP Snooping

The following example shows how to enable IGMP snooping.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip igmpsnooping
(Netgear Switch) (Config)#ip igmpsnooping interfacemode
(Netgear Switch) (Config)#exit
```

Example #2: show igmpsnooping

```
(Netgear Switch)     #show igmpsnooping?

<cr>           Press Enter to execute the command.
<slot/port>    Enter interface in slot/port format.
mrouter        Display IGMP Snooping Multicast Router information.
<1-4093>       Display IGMP Snooping valid VLAN ID information.

(Netgear Switch)     #show igmpsnooping

Admin Mode.............................        Enable
Multicast Control Frame Count..........        0
Interfaces Enabled for IGMP Snooping.....      1/0/10
Vlans enabled for IGMP snooping.........       20
```

Example #3: show mac-address-table igmpsnooping

```
(Netgear Switch) #show mac-address-table igmpsnooping ?

<cr>                      Press Enter to execute the command.

(Netgear Switch) #show mac-address-table igmpsnooping

                            Type       Description       Interfaces
----------------------    -------    --------------    -----------
00:01:01:00:5E:00:01:16    Dynamic    Network Assist    Fwd: 1/0/47
00:01:01:00:5E:00:01:18    Dynamic    Network Assist    Fwd: 1/0/47
00:01:01:00:5E:37:96:D0    Dynamic    Network Assist    Fwd: 1/0/47
00:01:01:00:5E:7F:FF:FA    Dynamic    Network Assist    Fwd: 1/0/47
00:01:01:00:5E:7F:FF:FE    Dynamic    Network Assist    Fwd: 1/0/47
```

Chapter 13
Port Security

This section describes the Port Security feature.

Overview

Port Security:

- Allows for limiting the number of MAC addresses on a given port
- Packets that have a matching MAC address (secure packets) are forwarded; all other packets (unsecure packets) are restricted
- Enabled on a per port basis
- When locked, only packets with allowable MAC address will be forwarded
- Supports both dynamic and static
- Implement two traffic filtering methods
  - Dynamic Locking - User specifies the maximum number of MAC addresses that can be learned on a port. The maximum number of MAC addresses is platform dependent and is given in the software Release Notes. After the limit is reached, additional MAC addresses are not learned. Only frames with an allowable source MAC address are forwarded.
  - Static Locking - User manually specifies a list of static MAC addresses for a port. Dynamically locked addresses can be converted to statically locked addresses.

  These methods can be used concurrently

Operation

Port Security:

- Helps secure network by preventing unknown devices from forwarding packets
- When link goes down, all dynamically locked addresses are ‘freed’
- If a specific MAC address is to be set for a port, set the dynamic entries to 0, then only allow packets with a MAC address matching the MAC address in the static list
- Dynamically locked MAC addresses are aged out if another packet with that address is not seen within the age-out time. The user can set the time-out value.
- Dynamically locked MAC addresses are eligible to be learned by another port
- Static MAC addresses are not eligible for aging
- Dynamically locked addresses can be converted to statically locked addresses

CLI Examples

The following are examples of the commands used in the Port Security feature.

Example #1: show port security

```
(Netgear Switch) #show port-security ?

<cr>                Press Enter to execute the command.
all                 Display port-security information for all interfaces.
<unit/slot/port>    Enter interface in unit/slot/port format.
dynamic             Display dynamically locked MAC addresses.
static              Display statically locked MAC addresses.
violation           Display the source MAC address of the last packet that
                    was discarded on a locked port.

(Netgear Switch) #show port-security

Port Security Administration Mode: Enabled
```

Example #2: show port security on a specific interface

```
(Netgear Switch) #show port-security 1/0/10

        Admin       Dynamic    Static        Violation
Intf    Mode        Limit      Limit         Trap Mode
----    --------    -------    ------        ---------
1/0/10  Disabled    600        20            Disabled
```

Example #3: (Config) port security

```
(Netgear Switch) (Config) #port-security ?

<cr>    Press Enter to execute the command.

(Netgear Switch) (Config) #port-security
```

Chapter 14
Traceroute

This section describes the Traceroute feature.

Use Traceroute to discover the routes that packets take when traveling on a hop-by-hop basis to their destination through the network.

- Maps network routes by sending packets with small Time-to-Live (TTL) values and watches the ICMP time-out announcements
- Command displays all L3 devices
- Can be used to detect issues on the network
- Tracks up to 20 hops
- Default UPD port used 33343 unless modified in the **traceroute** command

Note: You can execute Traceroute with CLI commands only—there is no Web interface for this feature.

CLI Example

The following shows an example of using the traceroute command to determine how many hops there are to the destination. The command output shows each IP address the packet passes through and how long it takes to get there. In this example, the packet takes 16 hops to reach its destination.

```
(Netgear Switch) #traceroute?
<ipaddr>      Enter IP address.

(Netgear Switch) #traceroute 216.109.118.74 ?
<cr>    Press Enter to execute the command.
<port>        Enter port no.

(Netgear Switch) #traceroute 216.109.118.74

Tracing route over a maximum of 20 hops

 1  10.254.24.1        40 ms       9 ms      10 ms
 2  10.254.253.1       30 ms      49 ms      21 ms
 3  63.237.23.33       29 ms      10 ms      10 ms
 4  63.144.4.1         39 ms      63 ms      67 ms
 5  63.144.1.141       70 ms      50 ms      50 ms
 6  205.171.21.89      39 ms      70 ms      50 ms
 7  205.171.8.154      70 ms      50 ms      70 ms
 8  205.171.8.222      70 ms      50 ms      80 ms
 9  205.171.251.34     60 ms      90 ms      50 ms
10  209.244.219.181    60 ms      70 ms      70 ms
11  209.244.11.9       60 ms      60 ms      50 ms
12  4.68.121.146       50 ms      70 ms      60 ms
13  4.79.228.2         60 ms      60 ms      60 ms
14  216.115.96.185    110 ms      59 ms      70 ms
15  216.109.120.203    70 ms      66 ms      95 ms
16  216.109.118.74     78 ms     121 ms      69 ms
```

Chapter 15
Configuration Scripting

This section describes the Configuration Scripting feature.

Overview

Configuration Scripting:

- Allows you to generate text-formatted files
- Provides scripts that can be uploaded and downloaded to the system
- Provides flexibility to create command configuration scripts
- May be applied to several switches
- Can save up to ten scripts or 500K of memory
- Provides List, Delete, Apply, Upload, Download
- Provides script format of one CLI command per line

Considerations

- Total number of scripts stored on box limited by NVRAM/FLASH size.
- Application of scripts is partial if script fails. For example, if the script executes five of ten commands and the script fails, the script stops at five.
- Scripts cannot be modified or deleted while being applied.
- Validation of scripts checks for syntax errors only. It does not validate that the script will run.

CLI Examples

The following are examples of the commands used for the Configuration Scripting feature.

Example #1: script

```
(Netgear Switch) #script ?

apply       Applies configuration script to the switch.
delete      Deletes a configuration script file from the switch.
list        Lists all configuration script files present on the switch.
show        Displays the contents of configuration script.
validate    Validate the commands of configuration script.
```

Example #2: script list and script delete

```
(Netgear Switch) #script list

Configuration Script Name        Size(Bytes)
-------------------------        -----------
basic.scr                        93
running-config.scr               3201

2 configuration script(s) found.
1020706 bytes free.

(Netgear Switch) #script delete basic.scr

Are you sure you want to delete the configuration script(s)? (y/n) y

1 configuration script(s) deleted.
```

Example #3: script apply running-config.scr

```
(Netgear Switch) #script apply running-config.scr

Are you sure you want to apply the configuration script? (y/n) y

The systems has unsaved changes.
Would you like to save them now? (y/n) y

Configuration Saved!
```

Example #4: Creating a Configuration Script

```
(Netgear Switch) #show running-config running-config.scr

Config script created successfully.

(Netgear Switch)                    #script list

Configuration Script Name        Size(Bytes)
-------------------------        ----------
running-config.scr               3201

1 configuration script(s) found.
1020799 bytes free.
```

Example #5: Upload a Configuration Script

```
(Netgear Switch) #copy nvram: script running-config.scr
tftp://192.168.77.52/running-config.scr

Mode.........................        TFTP
Set TFTP Server IP...........        192.168.77.52
TFTP Path....................        ./
TFTP Filename................        running-config.scr
Data Type....................        Config Script
Source Filename..............        running-config.scr

Are you sure you want to start? (y/n) y

File transfer operation completed successfully.
```

Chapter 16
Outbound Telnet

This section describes the Outbound Telnet feature.

Overview

Outbound Telnet:

- Establishes an outbound telnet connection between a device and a remote host
- A telnet connection is initiated, each side of the connection is assumed to originate and terminate at a “Network Virtual Terminal” (NVT)
- Server and user hosts do not maintain information about the characteristics of each other’s terminals and terminal handling conventions
- Must use a valid IP address

CLI Examples

The following are examples of the commands used in the Outbound Telnet feature.

Example #1: show network

```
(Netgear Switch Routing) >telnet 192.168.77.151
Trying 192.168.77.151...
(Netgear Switch Routing)
User:admin
Password:
(Netgear Switch Routing)    >en
Password:

(Netgear Switch Routing)    #show network

IP Address.............................. 192.168.77.151
Subnet Mask............................. 255.255.255.0
Default Gateway......................... 192.168.77.127
Burned In MAC Address................... 00:10:18.82.04:E9
Locally Administered MAC Address........ 00:00:00:00:00:00
MAC Address Type........................ Burned In
Network Configuration Protocol Current... DHCP
Management VLAN ID...................... 1
Web Mode................................ Enable
Java Mode .............................. Disable
```

Example #2: show telnet

```
(Netgear Switch Routing)#show telnet

Outbound Telnet Login Timeout (minutes)........ 5
Maximum Number of Outbound Telnet Sessions..... 5
Allow New Outbound Telnet Sessions............. Yes
```

Example #3: transport output telnet

```
(Netgear Switch Routing) (Config)#lineconfig ?

<cr>                      Press Enter to execute the command.

(Netgear Switch Routing) (Config)#lineconfig

(Netgear Switch Routing) (Line)#transport ?

input                     Displays the protocols to use to connect to a
                          specific line of the router.
output                    Displays the protocols to use for outgoing
                          connections from a line.

(Netgear Switch Routing) (Line)#transport output ?

telnet                    Allow or disallow new telnet sessions.

(Netgear Switch Routing) (Line)#transport output telnet ?

<cr>                      Press Enter to execute the command.

(Netgear Switch Routing) (Line)#transport output telnet

(Netgear Switch Routing) (Line)#
```

Example #4: session-limit and session-timeout

```
(Netgear Switch Routing) (Line)#session-limit ?

<0-5>                  Configure the maximum number of outbound telnet sessions
allowed.

(Netgear Switch Routing) (Line)#session-limit 5

(Netgear Switch Routing) (Line)#session-timeout ?

<1-160>                  Enter time in minutes.

(Netgear Switch Routing) (Line)#session-timeout 15
```

Chapter 17 Port Mirroring

This section describes the Port Mirroring feature.

Overview

Port Mirroring:

- Allows you to monitor network traffic with an external network analyzer
- Forwards a copy of each incoming and outgoing packet to a specific port
- Is used as a diagnostic tool, debugging feature or means of fending off attacks
- Assigns a specific port to copy all packets to
- Allows inbound or outbound packets to switch to their destination and to be copied to the mirrored port

CLI Examples

The following are examples of the commands used in the Port Mirroring feature.

Example #1: show monitor session

```
(Netgear Switch Routing) #show monitor session 1

Session ID    Admin Mode    Probe Port    Mirrored Port
----------    ----------    ----------    -------------
1             Enable        1/0/8         1/0/7
```

Note: Monitor session ID “1” - “1” is a hardware limitation.

Example #2: show port all

```
(Netgear Switch Routing) #show port all

                Admin     Physical    Physical    Link    Link     LACP
Intf    Type    Mode      Mode        Status      Status  Trap     Mode
----    ----    ------    --------    -------     ------  ----     ----
1/0/1           Enable    Auto                    Down    Enable   Enable
1/0/2           Enable    Auto                    Down    Enable   Enable
1/0/3           Enable    Auto                    Down    Enable   Enable
1/0/4           Enable    Auto                    Down    Enable   Enable
1/0/5           Enable    Auto                    Down    Enable   Enable
1/0/6           Enable    Auto                    Down    Enable   Enable
1/0/7    Mirror Enable    Auto                    Down    Enable   Enable
1/0/8    Probe  Enable    Auto                    Down    Enable   Enable
1/0/10          Enable    Auto                    Down    Enable   Enable
```

Example #3: show port interface

Use this command for a specific port. The output shows whether the port is the mirror or the probe

port, and what is enabled or disabled on the port.

```
(Netgear Switch Routing) #show port 0/7

                  Admin     Physical    Physical   Link      Link    LACP
Intf     Type     Mode      Mode        Status     Status    Trap    Mode
1/0/7    Mirror   Enable    Auto                   Down      Enable  Enable


(Netgear Switch Routing) #show port 0/8

                Admin     Physical    Physical        Link      Link    LACP
Intf    Type    Mode      Mode        Status          Status    Trap    Mode
----    ----    ------    --------    --------        ------    ----    ----
1/0/8   Probe   Enable    Auto                        Down      Enable  Enable
```

Example #4: (Config) monitor session 1 mode

To set up port mirroring, specify the monitor session, then the mode.

```
(Netgear Switch Routing)(Config)#monitor?
session    Configure port mirroring.

(Netgear Switch Routing)(Config)#monitor session?
<1-1>    Session number.

(Netgear Switch Routing)(Config)#monitor session 1?
destination    Configure the probe interface.
mode    Enable/Disable port mirroring session.
source    Configure the source interface.

(Netgear Switch Routing)(Config)#monitor session 1 mode?
<cr>    Press Enter to execute the command.
(Netgear Switch Routing)(Config)#monitor session 1 mode
```

Example #5: (Config) monitor session 1 source interface

Specify the source (mirrored) ports and destination (probe) port.

```
(Netgear Switch Routing)(Config)#monitor session 1 source?
interface    Configure interface.

(Netgear Switch Routing)(Config)#monitor session 1 source interface?
<slot/port>            Enter the interface.
(Netgear Switch Routing)(Config)#monitor session 1 source interface 0/7

(Netgear Switch Routing)(Config)#monitor session 1 destination?
interface    Configure interface.

(Netgear Switch Routing)(Config)#monitor session 1 destination interface?
<slot/port>            Enter the interface.
(Netgear Switch Routing)(Config)#monitor session 1 destination interface 0/8
```

Example #6: (Interface) port security

```
(Netgear Switch Routing)(Interface 0/7)#port-security ?

<cr>    Press Enter to execute the command.
mac-address    Add Static MAC address to the interface.
max-dynamic    Set Dynamic Limit for the interface.
max-static    Set Static Limit for the interface.

(Netgear Switch Routing)(Interface 0/7)#port-security max-static ?

<0-20>    Set Static Limit for the interface.

(Netgear Switch Routing)(Interface 0/7)#port-security max-static 5
(Netgear Switch Routing)(Interface 0/7)#port-security max-dynamic 10
```

Chapter 18
Simple Network Time Protocol (SNTP)

This section describes the Simple Network Time Protocol (SNTP) feature.

Overview

SNTP:

- Used for synchronizing network resources
- Adaptation of NTP
- Provides synchronized network timestamp
- Can be used in broadcast or unicast mode
- SNTP client implemented over UDP which listens on port 123

CLI Examples

The following are examples of the commands used in the SNTP feature.

Example #1: show sntp

```
(Netgear Switch Routing) #show sntp ?

<cr>      Press Enter to execute the command.
client    Display SNTP Client Information.
server    Display SNTP Server Information.
```

Example #2: show sntp client

```
(Netgear Switch Routing) #show sntp client

Client Supported Modes:    unicast broadcast
SNTP Version:              4
Port:                      123
Client Mode:               unicast
Unicast Poll Interval:     6
Poll Timeout (seconds):    5
Poll Retry:                1
```

Example #3: show sntp server

```
(Netgear Switch Routing) #show sntp server

Server IP Address:         81.169.155.234
Server Type:               ipv4
Server Stratum:            3
Server Reference Id:       NTP Srv: 212.186.110.32
Server Mode:               Server
Server Maximum Entries:    3
Server Current Entries:    1

SNTP Servers
------------

IP Address:                 81.169.155.234
Address Type:               IPV4
Priority:                   1
Version:                    4
Port:                       123
Last Update Time:           MAY 18 04:59:13 2005
Last Attempt Time:          MAY 18 11:59:33 2005
Last Update Status:         Other
Total Unicast Requests:     1111
Failed Unicast Requests:    361
```

Example #4: Configure SNTP

Netgear switches do not have a built-in real-time clock. However, it is possible to use SNTP to get the time from a public SNTP/NTP server over the Internet. You may need permission from those public time servers. The following steps configure SNTP on the switch:

1. Configure the SNTP server IP address. The IP address can be either from the public NTP server or your own. You can search the Internet to locate the public server. The servers available could be listed in domain-name format instead of address format. In that case, use the ping command on the PC to find the server's IP address. The following example configures the SNTP server IP address to 208.14.208.19.

```
(Netgear Switch) (Config)#sntp server 208.14.208.19
```

2. After configuring the IP address, enable SNTP client mode. The client mode may be either broadcast mode or unicast mode. If the NTP server is not your own, you must use unicast mode.

```
(Netgear Switch) (Config)#sntp client mode unicast
```

3. Once enabled, the client will wait for the polling interval to send the query to the server. The default value is approximately one minute. After this period, issue the show command to confirm the time has been received. The time will be used in all logging messages.

```
(Netgear Switch) #show sntp server
Server IP Address:                  208.14.208.19
Server Type:                        ipv4
Server Stratum:                     4
Server Reference Id:                NTP Srv: 208.14.208.3
Server Mode:                        Server
Server Maximum Entries:             3
Server Current Entries:             1
SNTP Servers
------------

IP Address: 208.14.208.19
Address Type: IPV4
Priority: 1
Version: 4
Port: 123
Last Update Time: Mar 26 03:36:09 2006
Last Attempt Time: Mar 26 03:36:09 2006
Last Update Status: Success
Total Unicast Requests: 2
Failed Unicast Requests: 0
```

Example #5: Setting Time Zone

The SNTP/NTP server is set to Coordinated Universal Time (UTC) by default. The following example shows how to set the time zone to Pacific Standard Time (PST) which is 8 hours behind GMT/UTC.

```
(Netgear switch)(config)#clock timezone PST -8
```

Example #6: Setting Named SNTP Server

Netgear provides SNTP servers accessible by Netgear devices.

Because Netgear may change IP addresses assigned to its time servers, it is best to access a SNTP server by DNS name instead of using a hard-coded IP address. The public time servers available are time-a, time-b, and time-c.

To use this feature, follow the steps below:

Enable a DNS name server and access a time server with the following commands:

```
(Netgear switch) (config)#ip domain-lookup
(Netgear switch) (config)#ip name-server 192.168.1.1
(Netgear switch) (config)#sntp server time-a.netgear.com
```

where “192.168.1.1” is the public network gateway IP address for your device.

This method of setting DNS name look-up can be used for any other applications that require a public IP address, for example, a RADIUS server.

Chapter 19
Syslog

This section provides information about the Syslog feature.

Overview

Syslog:

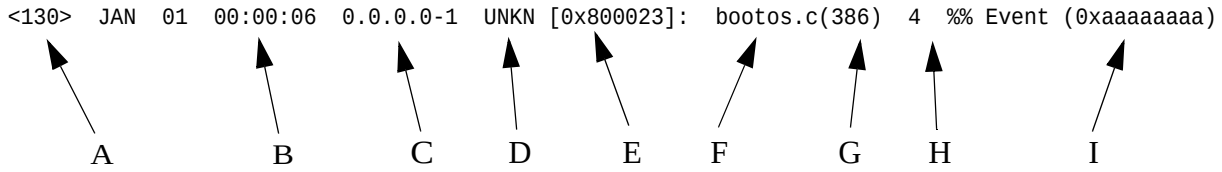
- Allows you to store system messages and/or errors
- Can store to local files on the switch or a remote server running a syslog daemon
- Method of collecting message logs from many systems

Persistent Log Files

- Currently three - one for each of the last three sessions
- Each log has two parts:
  - Start up log is the first 32 messages after system startup
  - Operational log is the last 32 messages received after the startup log is full
- Files are stored in ASCII format
  - slog0.txt - slog2.txt
  - olog0.txt - olog2.txt

    Where 0 is for the boot, 1 is for the last boot, 2 is for the boot before that; the third one overflows upon the next boot.
- Can be saved to local server to monitor at a later point in time

Interpreting Log Files



A. Priority

B. Timestamp

C. Stack ID

D. Component Name

E. Thread ID

F. File Name

G. Line Number

CLI Examples

The following are examples of the commands used in the Syslog feature.

Example #1: show logging

```
(Netgear Switch Routing) #show logging

Logging Client Local Port       :    514
CLI Command Logging             :    disabled
Console Logging                 :    disabled
Console Logging Severity Filter :    alert
Buffered Logging                :    enabled

Syslog Logging                  :    enabled

Log Messages Received           :    66
Log Messages Dropped            :    0
Log Messages Relayed            :    0
Log Messages Ignored            :    0
```

Example #2: show logging buffered

```
(Netgear Switch Routing) #show logging buffered ?

<cr>    Press Enter to execute the command.

(Netgear Switch Routing) #show logging buffered

Buffered (In-Memory) Logging          :    enabled
Buffered Logging Wrapping Behavior    :    On
Buffered Log Count                    :    66

<1> JAN 01 00:00:02 0.0.0.0-0 UNKN[268434944]: usmdb_sim.c(1205) 1 %% Error 0
(0x0)
<2> JAN 01 00:00:09 0.0.0.0-1 UNKN[268434944]: bootos.c(487) 2 %% Event
(0xaaaaaaaa)
<6> JAN 01 00:00:09 0.0.0.0-1 UNKN[268434944]: bootos.c(531) 3 %% Starting
code...
<6> JAN 01 00:00:16 0.0.0.0-3 UNKN[251627904]: cda_cnfgr.c(383) 4 %% CDA:
Creating new STK file.
<6> JAN 01 00:00:39 0.0.0.0-3 UNKN[233025712]: edb.c(360) 5 %% EDB Callback:
Unit Join: 3.
<6> JAN 01 00:00:40 0.0.0.0-3 UNKN[251627904]: sysapi.c(1864) 6 %% File
user_mgr_cfg: same version (6) but the sizes (2312->7988) differ
```

Example #3: show logging traplogs

```
(Netgear Switch Routing)                    #show logging traplogs         ?

<cr>    Press Enter to execute the command.

(Netgear Switch Routing)                    #show logging traplogs

Number of Traps Since Last Reset.............               6
Trap Log Capacity............................               256
Number of Traps Since Log Last Viewed.......                6

Log System Up Time         Trap
--- --------------         ------------------------------------------------
0   0 days 00:00:46        Link Up: Unit: 3 Slot: 0 Port: 2
1   0 days 00:01:01        Cold Start: Unit: 0
2   0 days 00:21:33        Failed User Login: Unit: 1 User ID: admin
3   0 days 18:33:31        Failed User Login: Unit: 1 User ID: \
4   0 days 19:27:05        Multiple Users: Unit: 0     Slot: 3 Port: 1
5   0 days 19:29:57        Multiple Users: Unit: 0     Slot: 3 Port: 1
```

Example #4: show logging hosts

```
(Netgear Switch Routing) #show logging hosts ?

<cr>                     Press Enter to execute the command.

(Netgear Switch Routing) #show logging hosts

Index     IP Address       Severity   Port     Status
-----  -----------------  ----------  ----  -------------
1      192.168.21.253     critical    514   Active
```

Example #5: logging port configuration

```
(Netgear Switch Routing)     #config

(Netgear Switch Routing) (Config)#logging ?

buffered          Buffered (In-Memory) Logging Configuration.
cli-command       CLI Command Logging Configuration.
console           Console Logging Configuration.
host              Enter IP Address for Logging Host
syslog            Syslog Configuration.

(Netgear Switch Routing) (Config)#logging host ?

<hostaddress>        Enter Logging Host IP Address
reconfigure          Logging Host Reconfiguration
remove               Logging Host Removal

(Netgear Switch Routing) (Config)#logging host 192.168.21.253 ?

<cr>             Press Enter to execute the command.
<port>           Enter Port Id

(Netgear Switch Routing) (Config)#logging host 192.168.21.253 4 ?

<cr>             Press Enter to execute the command.
<severitylevel>  Enter Logging Severity Level (emergency|0, alert|1,
critical|2, error|3, warning|4, notice|5, info|6, debug|7).

(Netgear Switch Routing) (Config)#logging host 192.168.21.253 4 1 ?

<cr>             Press Enter to execute the command.

(Netgear Switch Routing) (Config)#logging host 192.168.21.253 4 1

(Netgear Switch Routing) #show logging hosts

Index     IP Address       Severity   Port     Status
-----  ----------------  ----------  ----  -------------
1      192.168.21.253     alert       4     Active
```

Chapter 20
Managing Switch Stacks

This chapter describes the concepts and recommended operating procedures to manage Netgear stackable managed switches running Release 4.x.x.x or newer. Netgear stackable managed switches include the following models:

- FSM7328S
- FSM7352S
- FSM7352PS
- GSM7328S
- GSM7352S

Note: The FSM family and GSM family cannot be stacked together at this point.

This chapter includes the following topics:

- Initial installation and power-up of a stack
- Removing a unit from the stack
- Adding a unit to an operating stack
- Replacing a stack member with an new unit
- Renumbering stack members
- Moving the master to a different unit in the stack
- Removing a master unit from an operating stack
- Merging two operational stacks
- Pre configuration
- Upgrading firmware
- Migration of configuration with a firmware upgrade

Understanding Switch Stacks

A *switch stack* is a set of up to eight Ethernet switches connected through their stacking ports. One of the switches controls the operation of the stack and is called the stack master. The *stack master* and the other switches in the stack are *stack members*. The stack members use stacking technology to behave and work together as a unified system. Layer 2 and Layer 3 protocols present the entire switch stack as a single entity to the network.

The stack master is the single point of stack-wide management. From the stack master, you configure:

- System-level (global) features that apply to all stack members
- Interface-level features for all interfaces on any stack member

A switch stack is identified in the network by its network IP address. The network IP address is assigned according to the MAC address of the stack master. Every stack member is uniquely identified by its own *stack member number.*

All stack members are eligible stack masters. If the stack master becomes unavailable, the remaining stack members participate in electing a new stack master from among themselves. A set of factors determine which switch is elected the stack master. These factors are:

1. The switch that is master always has priority to retain the role of master
2. Assigned priority
3. MAC address

If the master cannot be selected by (1), then (2) is used. If (2) does not resolve which stack member becomes stack master, then (3) is used.

The stack master contains the saved and running configuration files for the switch stack. The configuration files include the system-level settings for the switch stack and the interface-level settings for all stack members. Each stack member retains a copy of the saved file for backup purposes.

If the master is removed from the stack, another member will be elected master, and will then run from that saved configuration.

You can use these methods to manage switch stacks:

- Stack web interface
- Command line interface (CLI) over a serial connection to the console port of the master
- A network management application through the Simple Network Management Protocol (SNMP)

Switch Stack Membership

A switch stack has up to eight stack members connected through their stacking ports. A switch stack always has one stack master.

A standalone switch is a switch stack with one stack member that also operates as the stack master. You can connect one standalone switch to another to create a switch stack containing two stack members, with one of them being the stack master. You can connect standalone switches to an existing switch stack to increase the stack membership.

If you replace a stack member with an identical model, the new switch functions with exactly the same configuration as the replaced switch, assuming that the new switch is using the same member number as the replaced switch. For information about the benefits of preconfiguring a switch stack, see “Preconfiguration” on page 20-15.

The operation of the switch stack continues uninterrupted during membership changes unless you remove the stack master or you add powered-on standalone switches or switch stacks.

- Adding powered-on switches (merging) causes the stack masters of the merging switch stacks to elect a stack master from among themselves. The re-elected stack master retains its role and configuration and so do its stack members. All remaining switches, including the former stack masters, reload and join the switch stack as stack members. They change their stack member numbers to the lowest available numbers and use the stack configuration of the re-elected stack master. Therefore, when you merge two powered stacks, you cannot control which unit becomes stack master and which configuration is used. For these reasons, it is recommended that powered switches be powered down before adding to an existing operating stack.
- Removing powered-on stack members can cause the switch stack to divide (partition) into two or more switch stacks, each with the same configuration. However, if cabled properly, the switch stack should not divide.
    - If the switch stack divides, and you want the switch stacks to remain separate, change the IP address or addresses of the newly created switch stacks.
    - If you did not intend to partition the switch stack:
        - Power off the newly created switch stacks
        - Reconnect them to the original switch stack through their stacking ports
        - Power on the switches

Switch Stack Cabling (FSM73xxS)

Figure 20-1 and Figure 20-2 illustrate how individual switches are interconnected to form a stack. You can use the regular Category 5 Ethernet 8 wire cable.

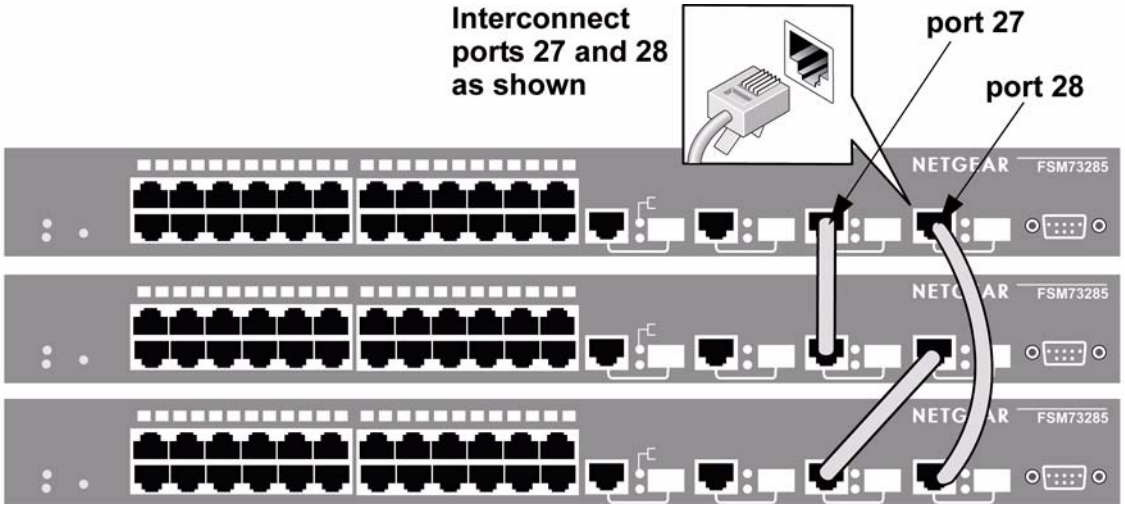


Figure 20-1

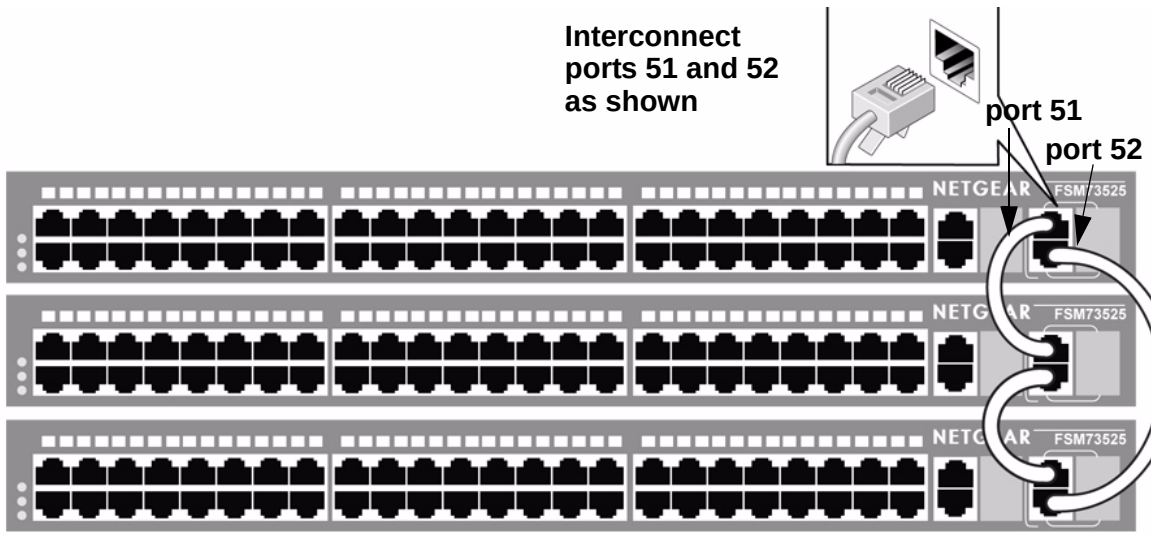


Figure 20-2

Stack Master Election and Re-Election

The stack master is elected or re-elected based on one of these factors and in the order listed:

1. The switch that is currently the stack master
2. The switch with the highest stack member priority value

Note: Netgear recommends assigning the highest priority value to the switch that you prefer to be the stack master. This ensures that the switch is re-elected as stack master if a re-election occurs.

3. The switch with the higher MAC address

A stack master retains its role unless one of these events occurs:

- The stack master is removed from the switch stack
- The stack master is reset or powered off
- The stack master has failed
- The switch stack membership is increased by adding powered-on standalone switches or switch stacks

In the case of a master re-election, the new stack master becomes available after a few seconds. In the meantime, the switch stack uses the forwarding tables in memory to minimize network disruption. The physical interfaces on the other available stack members are not affected while a new stack master is elected.

If a new stack master is elected and the previous stack master becomes available, the previous stack master does not resume its role as stack master.

Stack Member Numbers

A stack member number (1 to 8) identifies each member in the switch stack. The member number also determines the interface-level configuration that a stack member uses. You can display the stack member number by using the **show switch** user EXEC command.

A new, out-of-the-box switch (one that has not joined a switch stack or has not been manually assigned a stack member number) ships with a default stack member number of 1. When it joins a switch stack, its default stack member number changes to the lowest available member number in the stack.

Stack members in the same switch stack cannot have the same stack member number. Every stack member, including a standalone switch, retains its member number until you manually change the number or unless the number is already being used by another member in the stack.

See “Renumbering Stack Members” and “Merging Two Operational Stacks”.

Stack Member Priority Values

A stack member priority can be changed if the user would like change who is the master of the stack. Use the following command to change stack member's priority (this command is in the global config mode):

switch unit **priority** value

Switch Stack Offline Configuration

You can use the offline configuration feature to preconfigure (supply a configuration to) a new switch before it joins the switch stack. You can configure in advance the stack member number, the switch type, and the interfaces associated with a switch that is not currently part of the stack (see “Preconfiguration”

Effects of Adding a Preconfigured Switch to a Switched Stack

When you add a preconfigured switch to the switch stack, the stack applies either the preconfigured configuration or the default configuration. Table 20-1 lists the events that occur when the switch stack compares the preconfigured configuration with the new switch:

Table 20-1. Results of comparing the preconfiguration with the new switch

Scenario	Result
The stack member numbers and the switch types match. • If the stack member number of the preconfigured switch matches the stack member number in the configuration on the stack, and • If the switch type of the preconfigured switch matches the switch type in the configuration on the stack.	The switch stack applies the configuration to the preconfigured new switch and adds it to the stack.
The stack member numbers match but the switch types do not match. • If the stack member number of the preconfigured switch matches the stack member number in the configuration on the stack, but • The switch type of the preconfigured switch does not match the switch type in the configuration on the stack.	• The switch stack applies the default configuration to the preconfigured switch and adds it to the stack. • The configuration in the preconfigured switch is changed to reflect the new information.
The stack member number is not found in the configuration.	• The switch stack applies the default configuration to the new switch and adds it to the stack. • The preconfigured information is changed to reflect the new information.
The stack member number of the preconfigured switch is not found in the configuration.	The switch stack applies the default configuration to the preconfigured switch and adds it to the stack.

Effects of Replacing a Preconfigured Switch in a Switch Stack

When a preconfigured switch in a switch stack fails, is removed from the stack, and is replaced with another switch, the stack applies either the preconfiguration or the default configuration to it. The events that occur when the switch stack compares the configuration with the preconfigured switch are the same as those described in “Effects of Adding a Preconfigured Switch to a Switched Stack”.

Effects of Removing a Preconfigured Switch from a Switch Stack

If you remove a preconfigured switch from the switch stack, the configuration associated with the removed stack member remains in the running configuration as configured information. To completely remove the configuration, use the **no member** *unit_number* (this is in the stacking configuration mode).

Switch Stack Software Compatibility Recommendations

All stack members must run the same software version to ensure compatibility between stack members. The software versions on all stack members, including the stack master, must be the same. This helps ensure full compatibility in the stack protocol version among the stack members.

If a stack member is running a software version that is not the same as the stack master, then the stack member is not allowed to join the stack. Use the **show switch** command to list the stack members and software versions. See "Code Mismatch".

Incompatible Software and Stack Member Image Upgrades

You can upgrade a switch that has an incompatible software image by using the **archive download-sw** xmodem | ymodem | zmodem | tftp://*ip/filepath/filename* command (this is in the stacking configuration mode). It copies the software image from an existing stack member to the one with incompatible software. That switch automatically reloads and joins the stack as a fully functioning member.

Switch Stack Configuration Files

The configuration files record settings for all global and interface specific settings that define the operation of the stack and individual members. Once a **save config** command is issued, all stack members store a copy of the configuration settings. If a stack master becomes unavailable, any stack member assuming the role of stack master will operate from the saved configuration files.

When a new, out-of-box switch joins a switch stack, it uses the system-level settings of that switch stack. However, if you want it to store this system level configuration, you must issue a **save config** command.

You back up and restore the stack configuration in the same way as you would for standalone switch configuration by using the copy command.

Switch Stack Management Connectivity

You manage the switch stack and the stack member interfaces through the stack master. You can use the web interface, the CLI, and SNMP. You cannot manage stack members on an individual switch basis.

Connectivity to the Switch Stack Through Console Ports

You can connect to the stack master through the console port of the stack master only.

Connectivity to the Switch Stack Through Telnet

You can connect to the stack master by using a Telnet connection to the IP address of the stack.

Switch Stack Configuration Scenarios

Table 20-2 provides switch stack configuration scenarios. Most of the scenarios assume at least two switches are connected through their stacking ports.

Table 20-2. Switch stack configuration scenarios

Scenario	Result
Stack master election specifically determined by existing stack masters **Note**: This is not recommended. • Connect two powered-on switch stacks through the stacking ports.	Only one of the two stack masters becomes the new stack master. None of the other stack members become the stack master.
Stack master election specifically determined by the stack member priority value • Connect two switches through their stacking ports. • Use the **switch** *stack-member-number* **priority** *new-priority-number* global configuration command to set one stack member to a higher member priority value. • Restart both stack members at the same time.	The stack member with the higher priority value is elected stack master.

Table 20-2. Switch stack configuration scenarios (continued)

Scenario	Result
Stack master election specifically determined by the MAC address • Assuming that both stack members have the same priority value and software image, restart both stack members at the same time.	The stack member with the higher MAC address is elected stack master.
Add a stack member • Power off the new switch • Through their stacking ports, connect the new switch to a powered-on switch stack. • Power on the new switch.	The stack master is retained. The new switch is added to the switch stack.
Stack master failure • Remove (or power off) the stack master.	Based on "Stack Master Election and Re-Election", one of the remaining stack members becomes the new stack master. All other stack members in the stack remain as stack members and do not reboot.

Stacking Recommendations

The purpose of this section is to collect notes on recommended procedures and expected behavior of stacked managed switches. Procedures addressed initially are listed below.

- Initial installation and power-up of a stack.
- Removing a unit from the stack
- Adding a unit to an operating stack
- Replacing a stack member with a new unit
- Renumbering stack members
- Moving the master to a different unit in the stack
- Removing a master unit from an operating stack
- Merging two operational stacks
- Preconfiguration
- Upgrading firmware
- Migration of configuration with a firmware upgrade

General Practices

- When issuing a command (such as move management, or renumber), it is recommended that the command has fully completed before issuing the next command. For example, if a reset is issued to a stack member, use the **show port** command to verify that the unit has re-merged with the stack, and all ports are joined before issuing the next command.
- When physically removing or relocating a unit, always power down the unit before disconnecting stack cables.
- When reconnecting stack cables, connect them before powering up the unit, if possible, and insure a good connection by tightening all connector screws (where applicable).

Initial installation and Power-up of a Stack

1. Install units in rack.
2. Install all stacking cables. Fully connect, including the redundant stack link. It is highly recommended that a redundant link be installed.
3. Identify the unit to be the master. Power this unit up first.
4. Monitor the console port. Allow this unit to come up to the login prompt. If unit has the default configuration, it should come up as unit #1, and will automatically become a master unit. If not, renumber as desired.
5. If desired, preconfigure other units to be added to the stack. Preconfiguration is described in Section "Preconfiguration".
6. Power on a second unit, making sure it is adjacent (next physical unit in the stack) to the unit already powered up. This will insure the second unit comes up as a member of the stack, and not a "Master" of a separate stack.
7. Monitor the master unit to see that the second unit joins the stack. Use the "show switch" command to determine when the unit joins the stack. It will be assigned a unit number (unit #2, if it has the default configuration).
8. Renumber this stack unit, if desired. See section "Renumbering Stack Members" on recommendations for renumbering stack members.
9. Repeat steps 6 through 8 to add additional members to the stack. Always power on a unit adjacent to the units already in the stack.

Removing a Unit from the Stack

1. Make sure the redundant stack connection is in place and functional. All stack members should be connected in a logical ring.
2. Power down the unit to be removed.
3. Disconnect stack cables.
4. If unit is not to be replaced, reconnect the stack cable from the stack member above to the stack member below the unit being removed.
5. Remove unit from the rack.
6. If desired, remove the unit from the configuration by issuing the command:
   no member <unit-id>

Adding a Unit to an Operating Stack

1. Make sure the redundant stack connection is in place and functional. All stack members should be connected in a logical ring.
2. Preconfigure the new unit, if desired.
3. Install new unit in the rack. (Assumes installation below the bottom-most unit, or above the top-most unit).
4. Disconnect the redundant stack cable that connects the last unit in the stack back up to the first unit in the stack at the position in the ring where the new unit is to be inserted.
5. Connect this cable to the new unit, following the established order of “stack up” to “stack down” connections
6. Power up the new unit. Verify, by monitoring the master unit console port, that the new unit successfully joins the stack by issuing the **show switch** command. The new unit should always join as a “member” (never as master; the existing master of the stack should not change).
7. If the code version of the newly added member is not the same as the existing stack, update the code as described in section “Upgrading Firmware”.

Replacing a Stack Member with a New Unit

There are two possible situations here. First, if you replace a stack member of a certain model number with another unit of the same model, follow the process below:

- Follow the process in section “Removing a Unit from the Stack” to remove the desired stack member.
- Follow the process in section “Adding a Unit to an Operating Stack” to add a new member to the stack with the following exceptions:
  - Insert the new member in the same position in the stack as the one removed.
  - Preconfiguration described in step “Preconfigure the new unit, if desired.” of that procedure is not required.

Second, if you replace a stack member with another unit of a different model number, use the following process:

- Follow the process in section “Removing a Unit from the Stack” to remove the desired stack member.
- Remove the now-absent stack member from the configuration by issuing the command **no member** command.

- Add the new stack unit to the stack using the process described in section "Adding a Unit to an Operating Stack". The unit can be inserted into the same position as the unit just removed, or the unit can be inserted at the bottom of the stack. In either case, make sure all stack cables are connected with the exception of the cable at the position where the new unit is to be inserted to insure that the stack does not get divided into two separate stacks, causing the election of a new master.

Renumbering Stack Members

1. If particular numbering is required, it is recommended that stack members be assigned specific numbers when they are first installed and configured in the stack, if possible.
2. If the desired stack unit number for a particular unit is unused, a unit can be renumbered simply by using the **switch** <oldunit-id> **renumber** <newunit-id> CLI command. This command is found in global config mode.
3. If the newunit-id has been preconfigured, you may need to remove the newunit-id from the configuration before renumbering the unit.
4. If reassignment of multiple existing stack unit numbers is necessary, there are a number of implications in terms of mismatching of configuration. In this case, it is recommended that all units except the master be powered down and added back one at a time using the procedure in Section "Adding a Unit to an Operating Stack".

Moving a Master to a Different Unit in the Stack

1. Using the **movemanagement** command, move the master to the desired unit number. The operation may take between 30 seconds and 3 minutes depending on the stack size and configuration. The command is **movemanagement** <fromunit-id> <tounit-id>
2. Make sure that you can log in on the console attached to the new master. Use the **show switch** command to verify that all units rejoined the stack.
3. It is recommended that the stack be reset with the **reload** command after moving the master.

Removing a Master Unit from an Operating Stack

1. First, move the designated master to a different unit in the stack using "Moving a Master to a Different Unit in the Stack".
2. Second, using "Removing a Unit from the Stack", remove the unit from the stack.

Merging Two Operational Stacks

It is strongly recommended that two functioning stacks (each having an independent master) not be merged simply by the reconnection of stack cables. That process may result in a number of unpredictable results and should be avoided.

1. Always power off all units in one stack before connecting into another stack.
2. Add the units as a group by unplugging one stacking cable in the operational stack and physically connecting all unpowered units at that point.
3. Completely cable the stacking connections, making sure the redundant link is also in place.
4. Then, power up each unit, one at a time, by following “Adding a Unit to an Operating Stack”.

Preconfiguration

All configuration on the stack except unit numbers is stored on the management unit. This means that a stack unit may be replaced with another device of the same type without having to reconfigure the switch. Unit numbers are stored independently on each switch, so that after power cycling the stack the units always come back with the same unit numbers. The unit type associated with each unit number may be learned by the management unit automatically as the units are connected or preconfigured by the administrator.

1. Issue the **member** <unit-id> <switchindex> command to preconfigure a unit. Supported unit types are shown by the **show supported switchtype** command.
2. Next, configure the unit you just defined with configuration commands, just as if the unit were physically present.
3. Ports for the preconfigured unit come up in “detached” state and can be seen with the **show port all** command. The detached ports may now be configured for VLAN membership and any other port-specific configuration.
4. After a unit type is preconfigured for a specific unit number, attaching a unit with different unit type for this unit number causes the switch to report an error. The **show switch** command indicates “config mismatch” for the new unit and the ports on that unit don’t come up. To resolve this situation the customer may change the unit number of the mismatched unit or delete the preconfigured unit type using the **no member** <unit-id> command.

Upgrading Firmware

New code is downloaded via TFTP or xmodem to the management unit using the **copy** command. Once code is successfully loaded on the management unit, it automatically propagates the code to the other units in the stack. If some error occurs during code propagation to stack units then the

archive command (in stack configuration mode) may be issued to make another attempt to copy the software to the unit(s) that did not get updated. Errors during code propagation to stack members could be caused by stack cable movement or unit reconfiguration during the propagation phase. An error could also occur in the presence of excessive network traffic (such as a broadcast event).

All units in the stack must run the same code version. Ports on stack units that don't match the management unit code version don't come up and the **show switch** command shows a "code mismatch" error. To resolve this situation the administrator may issue **archive** command. This command copies management unit's software to the other units with mismatched code version. Before issuing this command, be sure the code running on the management unit is the desired code revision for all units in the stack. Once code is loaded to all members of the stack, the units must be reset in order for the new code to start running.

Migration of Configuration With a Firmware Upgrade

In some cases, a configuration may not be carried forward in a code update. For updates where this issue is to be expected, the following procedure should be followed:

1. Save the current configuration by uploading it from the stack, using the copy command from the CLI.
2. Load new code into the stack manager. Reboot the stack.
3. Upon reboot, go into the boot menu and erase the configuration ("restore to factory defaults")
4. Continue with boot of operational code.
5. Once the stack is up, download the saved configuration back to the master. This configuration should then be automatically propagated to all members of the stack

Code Mismatch

If a unit is added to a stack and it does not have the same version of code as that of the master, the following should happen:

- "New" unit will boot up and become a "member" of the stack
- Ports on the added unit should remain in the "detached" state
- A message should appear on the CLI indicating a code mismatch with the newly added unit.
- To have the newly added unit to merge normally with the stack, code should be loaded to the newly added unit from the master using the copy command. The newly added member should then be reset, and should reboot normally and join the stack.

Chapter 21
Pre-Login Banner

This section describes the Pre-Login Banner feature.

Overview

Pre-Login Banner:

- Allows you to create message screens when logging into the CLI Interface
- By default, no Banner file exists
- Can be uploaded or downloaded
- File size cannot be larger than 2K

The Pre-Login Banner feature is only for the CLI interface.

CLI Example

Example 1#: Create a Pre-Login Banner

To create a Pre-Login Banner, follow these steps:

1. On your PC, using Notepad create a banner.txt file that contains the banner to be displayed.

```
Login Banner - Unauthorized access is punishable by law.
```

2. Transfer the file from the PC to the switch using TFTP

```
(Netgear Switch Routing) #copy tftp://192.168.77.52/banner.txt
nvram:clibanner

Mode..................................... TFTP
Set TFTP Server IP....................... 192.168.77.52
TFTP Path................................ ./
TFTP Filename............................ banner.txt
Data Type................................ Cli Banner

Are you sure you want to start? (y/n) y

CLI Banner file transfer operation completed successfully!

(Netgear Switch Routing)#exit

(Netgear Switch Routing) >logout

Login Banner - Unauthorized access is punishable by law.
User:
```

Note: The **no clibanner** command removes the banner from the switch.

Chapter 22
IGMP Querier

When the switch is used in network applications where video services such as IPTV, video streaming, and gaming are deployed, the video traffic would normally be flooded to all connected ports because such traffic packets usually have multicast Ethernet addresses. IGMP snooping can be enabled to create a multicast group to direct that traffic only to those users that require it.

However, the IGMP snooping operation usually requires an extra network device—normally a router—that can generate an IGMP membership query and solicit interested nodes to respond. With the build-in IGMP Querier feature inside the switch, such an external device is no longer needed.

Since the IGMP querier is designed to work with IGMP snooping, it is necessary to enable IGMP snooping when using it.

The examples in this chapter show how to setup the switch to generate the IGMP query.

Figure 22-1 shows a network application for video streaming service using the IGMP querier feature.

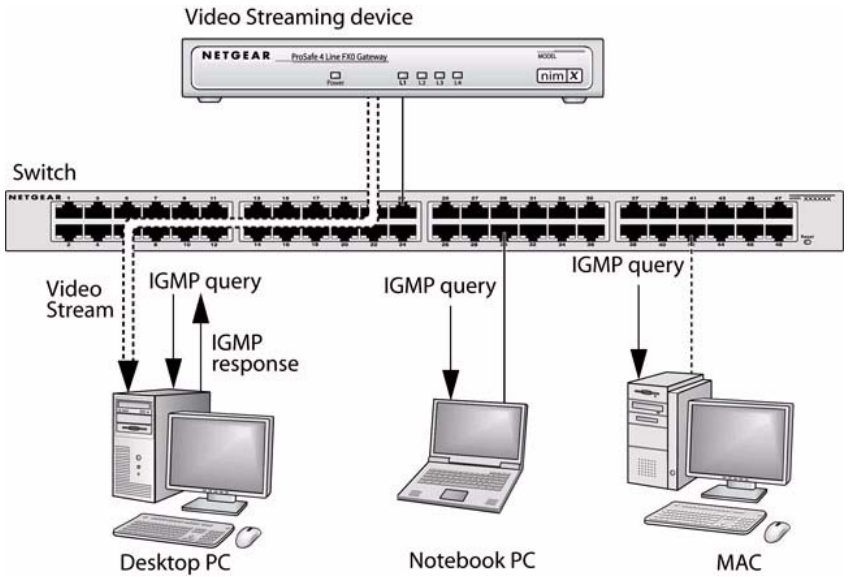


Figure 22-1

CLI Examples

Example #1: Enable IGMP Querier

Use the following CLI commands to set up the switch to generate IGMP querier packet for a designated VLAN. The IGMP packet will be transmitted to every ports on the VLAN. The following example enables the querier for VLAN 1. See the CLI Manual for more details about other IGMP querier command options.

```
(Netgear switch) #vlan database
(Netgear switch) (vlan)#ip igmp 1
(Netgear switch) (vlan)#ip igmpsnooping querier 1
(Netgear switch) (vlan)#exit
(Netgear switch) #config
(Netgear switch) (config)#ip igmpsnooping
(Netgear switch) (config)#exit
```

Example #2: Show IGMP Querier Status

To see the IGMP querier status, use the following command.

```
(Netgear switch) #show ip igmpsnooping querier 1

Vlan ID..................................... 1
Admin Mode.................................. Active
Query IP Address............................ 10.10.10.1
Querier Interval............................ 60
Query Packets Sent Count.................... 242
```

The command shows that the IGMP admin mode is Active. The mode is controlled by the **ip igmpsnooping** command. If the mode is inactive, no query packet is sent.

Chapter 23
DNS

This section describes the Domain Name System (DNS) feature. The DNS protocol maps a host name to an IP address, allowing you to replace the IP address with the host name for IP commands such as a ping and a traceroute, and for features such as RADIUS, DHCP Relay, SNTP, SNMP, TFTP, SYSLOG, and UDP Relay.

You can obtain the DNS server IP address from your ISP or public DNS server list.

Overview

DNS:

- Is used to resolve the host's IP address
- Enables a static host name entry to be used to resolve the IP address

Examples

The following are examples of how the DNS feature is used.

Example 1#: Specify Two DNS Servers

The following example shows how to specify two DNS servers (that is, two IP addresses for DNS servers) and to resolve an IP address using the DNS server.

The example is shown as CLI commands and as a Web interface procedure.

CLI Commands

To use the CLI to specify two DNS servers, enter the following CLI commands:

```
(Netgear Switch)#config
(Netgear Switch) (Config)#ip name-server 12.7.210.170 219.141.140.10
(Netgear Switch) (Config)#ip domain-lookup
(Netgear Switch) (Config)#exit
(Netgear Switch)#ping www.netgear.com

Send count=3, Receive count=3 from 206.82.202.46
```

Web Interface Procedure

To use the Web interface to specify two DNS servers, proceed as follows:

1. From the main menu, select System > Management > DNS > DNS Configuration. A screen similar to the following displays.

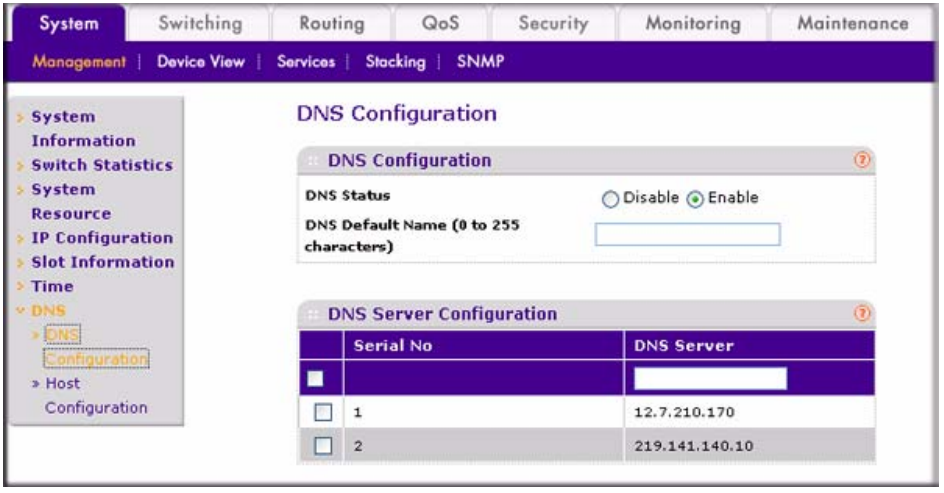


Figure 23-1

2. Under DNS Server Configuration, in the DNS Server field, enter **12.7.210.170**.
3. Click **Add**.
4. Under DNS Server Configuration, in the DNS Server field, enter **219.141.140.10**.
5. Click **Add**.

Both DNS servers now show in the DNS Server Configuration table.

Example 2#: Manually Add a Host Name and an IP Address

The following example shows commands to add a static host name entry to the switch so that you can use this entry to resolve the IP address.

The example is shown as CLI commands and as a Web interface procedure.

CLI Commands

To use the CLI to manually add a host name and an IP address, enter the following CLI commands:

```
(Netgear Switch)#config
(Netgear Switch) (Config)#ip host www.netgear.com 206.82.202.46
(Netgear Switch) (Config)#ip domain-lookup
(Netgear Switch) (Config)#ping www.netgear.com

Send count=3, Receive count=3 from 206.82.202.46
```

Web Interface Procedure

To use the Web interface to manually add a host name and an IP address, proceed as follows:

1. From the main menu, select System > Management > DNS > Host Configuration. A screen similar to the following displays.

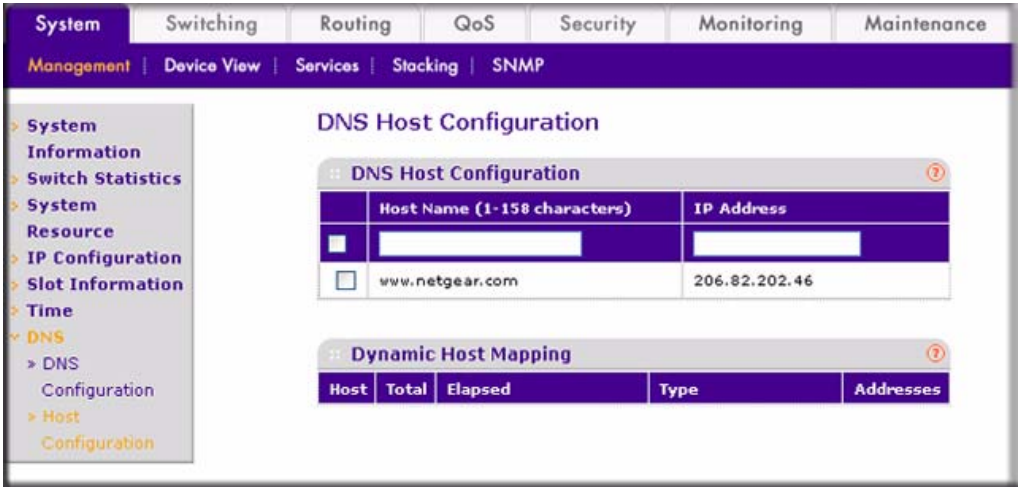


Figure 23-2

2. Under DNS Host Configuration, enter the following information:
   - In the Host Name field, enter **www.netgear.com**.
   - In the IP Address field, enter **206.82.202.46**.
3. Click **Add**.

The host name and IP address now show in the DNS Host Configuration table.

Chapter 24
DHCP Server

This section describes the DHCP server configuration. When a client sends a request to a DHCP server, the DHCP server assigns the IP address from address pools that are specified on the switch. The network in the DHCP pool must belong to the same subnet.

Overview

DHCP Server:

- Allows the switch to dynamically assign an IP address to a DHCP client that is attached to the switch
- Enables the IP address to be assigned based on the client's MAC address

Examples

The following are examples of how the DHCP Server feature is used.

Example 1#: Configure DHCP Server in Dynamic Mode

The following example shows how to create a DHCP server with a dynamic pool.

The example is shown as CLI commands and as a Web interface procedure.

CLI Commands

To use the CLI to create a DHCP server with a dynamic pool, enter the following CLI commands:

```
(Netgear Switch)#config
(Netgear Switch) (Config)#service dhcp
(Netgear Switch) (Config)#ip dhcp pool pool_dynamic
(Netgear Switch) (Config)#network 192.168.100.0 255.255.255.0
```

Web Interface Procedure

To use the Web interface to create a DHCP server with a dynamic pool, proceed as follows:

1. From the main menu, select System > Services > DHCP Server > DHCP Server Configuration. A screen similar to the following displays.

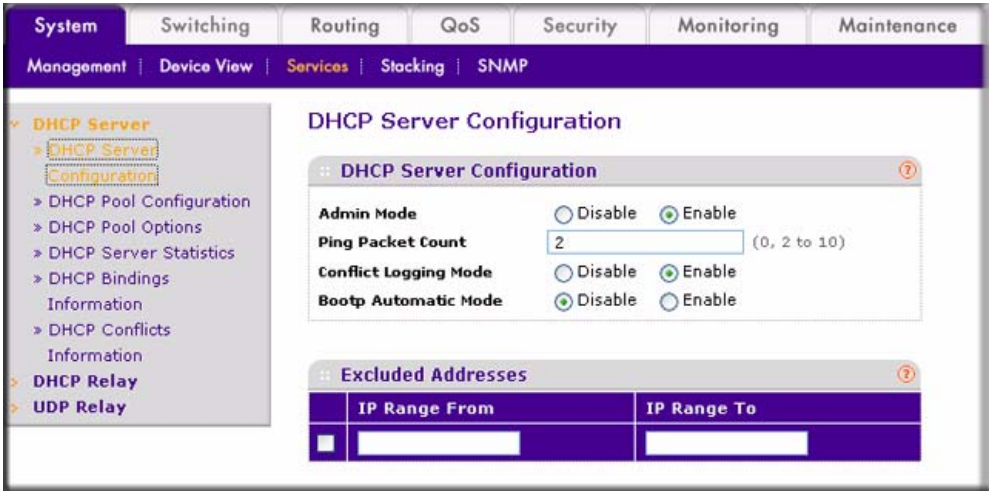


Figure 24-1

2. Next to Admin Mode, select the **Enable** radio button.
3. Click **Apply** to enable the DHCP service.

4. From the main menu, select System > Services > DHCP Server > DHCP Pool Configuration. A screen similar to the following displays.

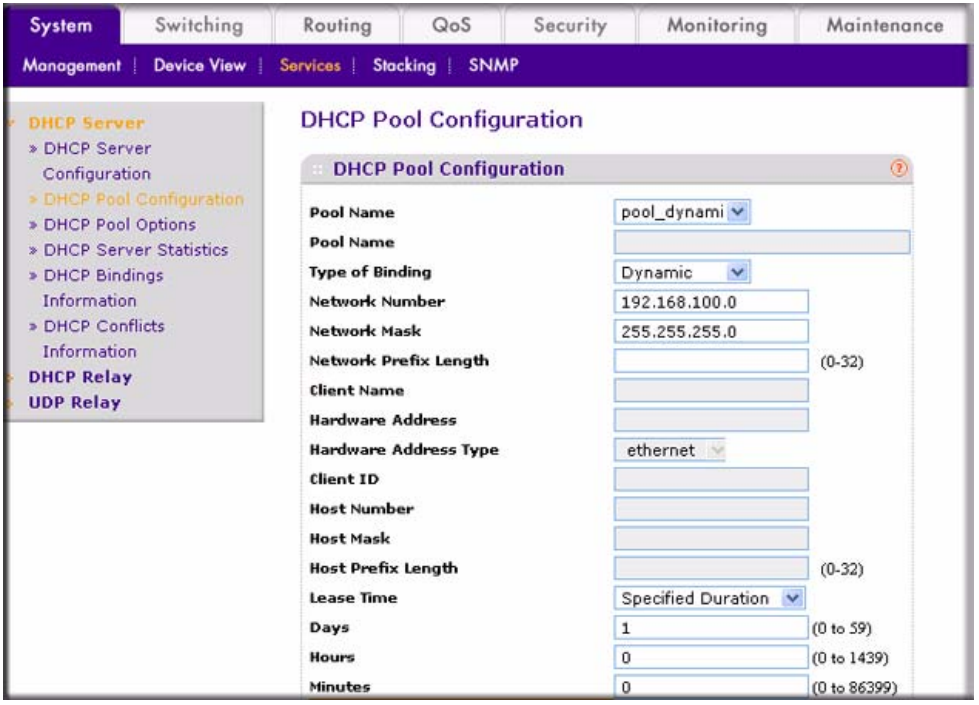


Figure 24-2

5. Under DHCP Pool Configuration, enter the following information:

- Select **Create** from the Pool Name pulldown menu.
- In the Pool Name field, enter **pool_dynamic**.
- Select **Dynamic** from the Type of Binding pulldown menu.
- In the Network Number field, enter **192.168.100.0**.
- In the Network Mask field, enter **255.255.255.0**. As an alternate, you can enter **24** in the Network Prefix Length field.
- In the Days field, enter **1**.

6. Click **Add**. The pool_dynamic name is now added to the Pool Name pulldown menu.

Example #2: Configure a DHCP Server in Manual Mode

The following example shows how to create a DHCP server with a manual pool.

The example is shown as CLI commands and as a Web interface procedure.

CLI Commands

To use the CLI to create a DHCP server with a with a manual pool, enter the following CLI commands:

```
(Netgear Switch)#config
(Netgear Switch) (Config)#service dhcp
(Netgear Switch) (Config)#ip dhcp pool pool_manual
(Netgear Switch) (Config)#client-name dhcpclient
(Netgear Switch) (Config)#hardware-address 00:01:02:03:04:05
(Netgear Switch) (Config)#host 192.168.200.1 255.255.255.0
(Netgear Switch) (Config)#client-identifier 01:00:01:02:03:04:05
```

Note: The unique identifier is a concatenation of the media type and MAC addresses. For example, the Microsoft client identifier for Ethernet address c8:19:24:88:f1:77 is 01:c8:19:24:88:f1:77, where 01 represents the Ethernet media type. For more information, see the “Address Resolution Protocol Parameters” section of RFC 1700.

Web Interface Procedure

To use the Web interface to create a DHCP server with a manual pool, proceed as follows:

1. From the main menu, select System > Services > DHCP Server > DHCP Server Configuration. A screen similar to the following displays.

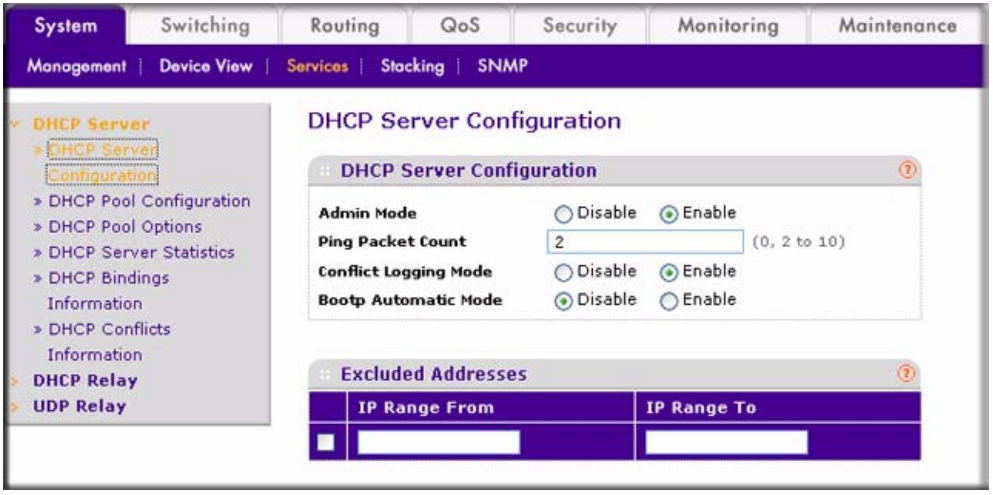


Figure 24-3

1. Next to Admin Mode, select the **Enable** radio button.
2. Click **Apply** to enable the DHCP service.
3. From the main menu, select System > Services > DHCP Server > DHCP Pool Configuration. A screen similar to the following displays.

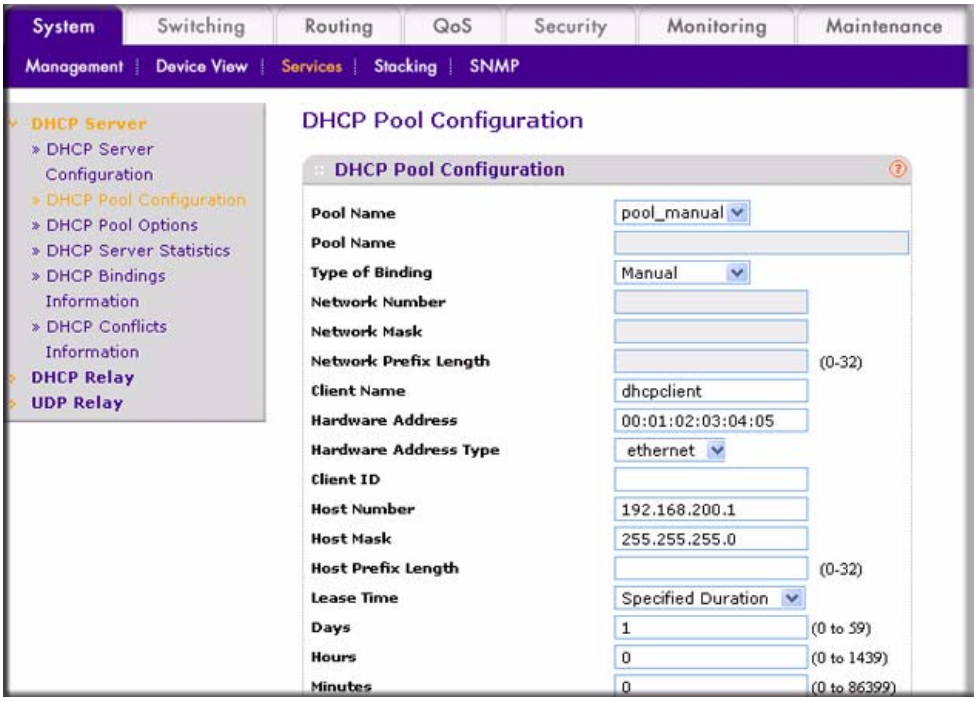


Figure 24-4

4. Under DHCP Pool Configuration, enter the following information:
   - Select **Create** from the Pool Name pulldown menu.
   - In the Pool Name field, enter **pool_manual**.
   - Select **Manual** from the Type of Binding pulldown menu.
   - In the Client Name field, enter **dhcpclient**.
   - In the Hardware Address field, enter **00:01:02:03:04:05**.
   - Select **ethernet** from the Hardware Type pulldown menu.
   - In the Host Number field, enter **192.168.200.1**.
   - In the Network Mask field, enter **255.255.255.0**. As an alternate, you can enter **24** in the Network Prefix Length field.
   - In the Days field, enter **1**.
5. Click **Add**. The pool_manual name is now added to the Pool Name pulldown menu.

Chapter 25
Protected Ports

This section describes how to set up protected ports on the switch. Some situations might require that traffic is prevented from being forwarded between any ports at Layer 2 so that one user cannot see the traffic of another user on the same switch.

Overview

Protected Ports:

- Prevent traffic from being forwarded between protected ports
- Allow traffic to be forwarded between a protected port and a non-protected port

Example

The following are examples of how the Protected Ports feature is used.

Example #1: Configure a Protected Port to Isolate Ports on the Switch

In following example, PC1 and PC2 can access the Internet as usual, but PC1 cannot see the traffic that is generated by PC2, that is, no traffic is forwarded between PC1 and PC2.

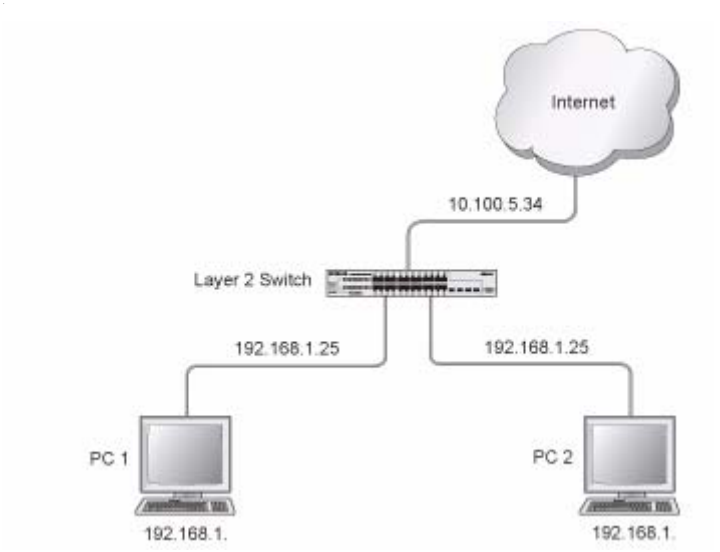


Figure 25-1

The example is shown as CLI commands and as a Web interface procedure.

CLI Commands

To use the CLI to configure a protected port in order to isolate ports, enter the following CLI commands:

```
Step 1: Create one VLAN 192 including PC1 and PC2.
(Netgear Switch) #vlan database
(Netgear Switch) #vlan 192
(Netgear Switch) #vlan routing 192
(Netgear Switch) #exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/23
(Netgear Switch) (Interface 1/0/23)#vlan pvid 192
(Netgear Switch) (Interface 1/0/23)#vlan participation include 192
(Netgear Switch) (Interface 1/0/23)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 192
(Netgear Switch) (Interface 1/0/24)#vlan participation include 192
(Netgear Switch) (Interface 1/0/24)#exit
(Netgear Switch) (Interface-vlan 192)#interface vlan 192
(Netgear Switch) (Interface-vlan 192)#routing
(Netgear Switch) (Interface-vlan 192)#ip address 192.168.1.254 255.255.255.0
(Netgear Switch) (Interface-vlan 192)#exit
```

```
Step 2: Create one VLAN 202 connected to the Internet.
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 202
(Netgear Switch) (Vlan)#vlan routing 202
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan pvid 202
(Netgear Switch) (Interface 1/0/48)#vlan participation include 202
(Netgear Switch) (Interface 1/0/48)#exit
(Netgear Switch) (Config)#interface vlan 202
(Netgear Switch) (Interface-vlan 202)#routing
(Netgear Switch) (Interface-vlan 202)ip address 10.100.5.34 255.255.255.0
(Netgear Switch) (Interface-vlan 202)#exit

Step 3: Create a DHCP pool to allocate IP addresses to PCs.
(Netgear Switch) (config)#service dhcp
(Netgear Switch) (config)#ip dhcp pool pool-a
(Netgear Switch) (Config-dhcp-pool)#dns-server 12.7.210.170
(Netgear Switch) (Config-dhcp-pool)#default-router 192.168.1.254
(Netgear Switch) (Config-dhcp-pool)#network 192.168.1.0 255.255.255.0
(Netgear Switch) (Config-dhcp-pool)#exit

Step 4: Enable IProuting and Configure a default route.
(Netgear Switch)(config)#ip routing
(Netgear Switch)(config)#ip route 0.0.0.0 0.0.0.0 10.100.5.252

Step 5: Enable a protected port on 1/0/23 and 1/0/24.
(Netgear Switch) (Config)#interface 1/0/23
(Netgear Switch) (Interface 1/0/23)#switchport protected
(Netgear Switch) (Interface 1/0/23)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#switchport protected
(Netgear Switch) (Interface 1/0/24)#exit
```

Web Interface Procedure

To use the Web Interface to configure a protected port in order to isolate ports, proceed as follows:

1. Create a DHCP pool:

Note: This example assumes that the DHCP service is enabled. For information about how to enable the DHCP service, see the Web interface procedure in "Example 1#: Configure DHCP Server in Dynamic Mode" in Chapter 24

a. From the main menu, select System > Services > DHCP Server > DHCP Server Configuration. A screen similar to the following displays.

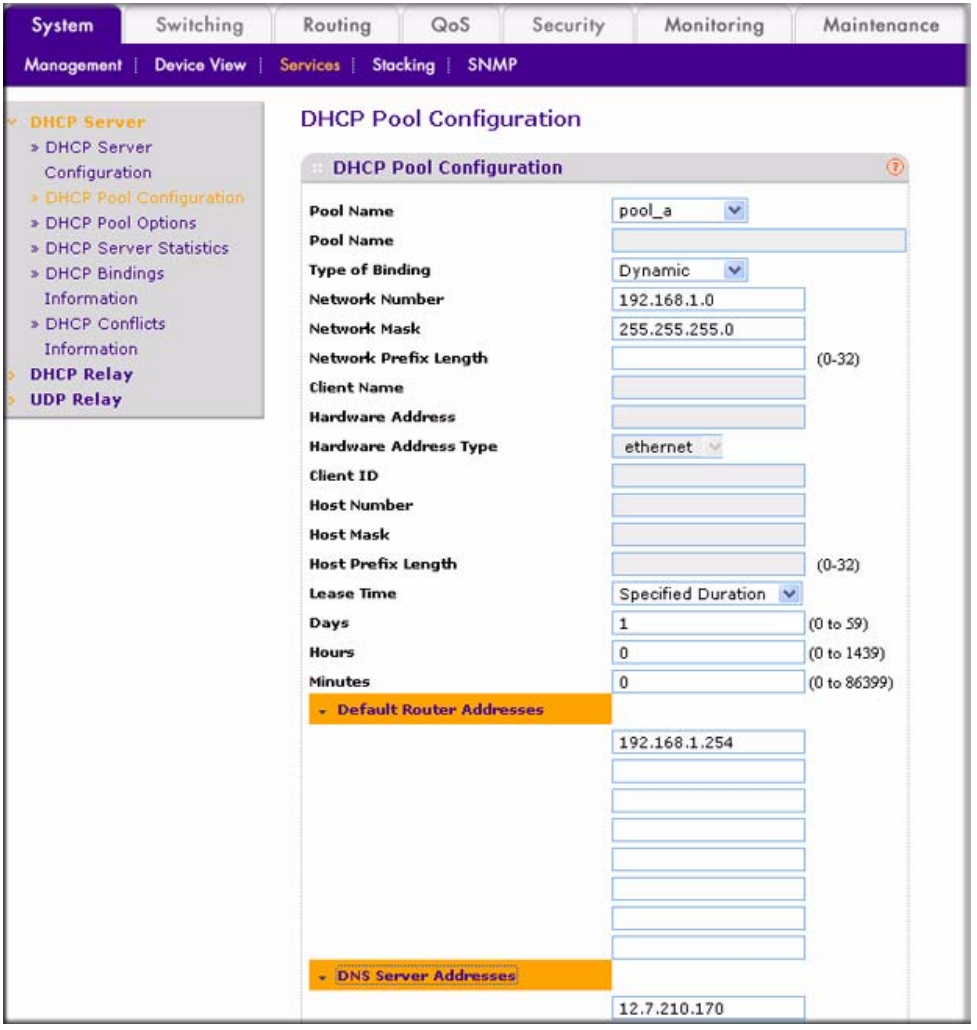


Figure 25-2

b. Under DHCP Pool Configuration, enter the following information:

- Select **Create** from the Pool Name pulldown menu.
- In the Pool Name field, enter **pool-a**.
- Select **Dynamic** from the Type of Binding pulldown menu.

- In the Network Number field, enter **192.168.1.0**.
- In the Network Mask field, enter **255.255.255.0**.
- In the Days field, enter **1**.
- Click on **Default Router Addresses**. The DNS server address fields display. In the first router address field, enter **192.168.1.254**.
- Click on **DNS Server Addresses**. The router address fields display. In the first DNS server address field, enter **12.7.210.170**.

c. Click **Add**.

2. Configure a VLAN and include ports 1/0/23 and 1/0/24 in the VLAN:

a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.

System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Routing Table | IP | VLAN | ARP | RIP | OSPF | Router Discovery | VRRP
VLAN Routing Wizard
VLAN Routing
VLAN Routing Wizard
VLAN Routing Wizard
Vlan ID
192
LAG Enabled
IP Address
192.168.1.254
Network Mask
255.255.255.0
Unit 1
Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
U U
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
49 50 51 52

Figure 25-3

b. Enter the following information in the VLAN Routing Wizard:

- In the Vlan ID field, enter **192**.
- In the IP Address field, enter **192.168.1.254**.
- In the Network Mask field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display:

- Click the gray box under port 23 twice until **U** displays.
- Click the gray box under port 24 twice until **U** displays.

The U specifies that the egress packet is untagged for the port.

d. Click **Apply** to save the VLAN that includes ports 23 and 24.

3. Configure a VLAN and include port 1/0/48 in the VLAN:

a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.

System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Routing Table | IP | VLAN | ARP | RIP | OSPF | Router Discovery | VRRP
VLAN Routing Wizard
VLAN Routing
VLAN Routing Wizard
VLAN Routing Wizard
Vlan ID
202
LAG Enabled
IP Address
10.100.5.34
Network Mask
255.255.255.0
Unit 1
Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
U
49 50 51 52

Figure 25-4

b. Enter the following information in the VLAN Routing Wizard:

- In the Vlan ID field, enter **202**.
- In the IP Address field, enter **10.100.5.34**.
- In the Network Mask field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display:

d. Click the gray box under port 48 twice until **U** displays. The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save the VLAN that includes port 48.

4. Enable IP Routing:

a. From the main menu, select Routing > IP > Basic > IP Configuration. A screen similar to the following displays.

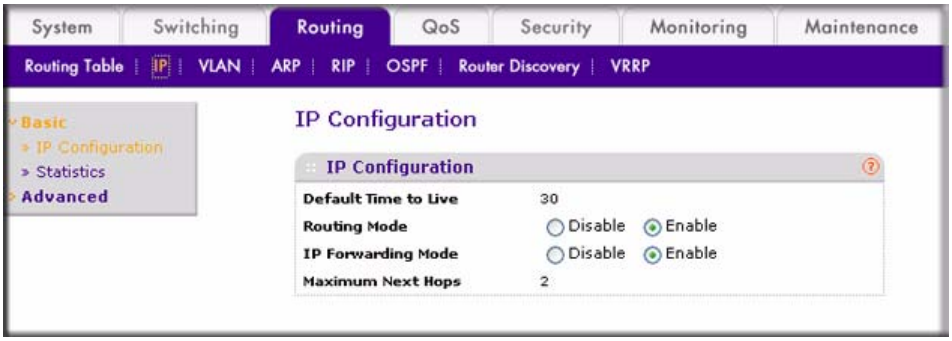


Figure 0-1

b. Under IP Configuration, make the following selections:

- Next to Routing Mode, select the **Enable** radio button.
- Next to IP Forwarding Mode, select the **Enable** radio button.

c. Click **Apply** to enable IP Routing.

5. Configure default route for VLAN 202:

a. From the main menu, select Routing > Routing Table > Basic > Route Configuration. A screen similar to the following displays.

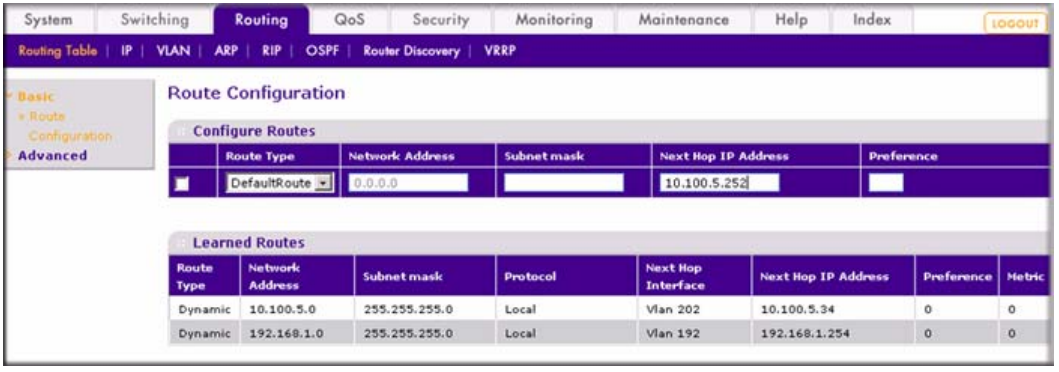


Figure 25-5

b. Under Configure Routes, select **DefaultRoute** from the Route Type pulldown menu.

c. Under Configure Routes, in the Next Hop IP Address field, enter **10.100.5.252**.

d. Click **Add** to add the route that is associated to VLAN 202 to the Learned Routes table.

6. Configure port 23 and port 24 as protected ports:

a. From the main menu, select Security > Traffic Control > Protected Port. A screen similar to the following displays.

System
Switching
Routing
QoS
Security
Monitoring
Maintenance
Help
Management Security | Access | Port Authentication | Traffic Control | ACL
MAC Filter
Storm Control
Port Security
Protected Port
Protected Ports Membership
Protected Port Membership
Unit 1
Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
49 50 51 52

Figure 25-6

b. Under Protected Ports Configuration, Click **Unit 1**. The ports display.

c. Click the gray box under ports 23. A flag appears in the box.

d. Click the gray box under ports 24. A flag appears in the box.

e. Click **Apply** to activate ports 23 and 24 as protected ports.

Chapter 26
802.1x Port Security

This section describes how to configure the 802.1x Port Security feature on a switch port. IEEE 802.1x authentication prevents unauthorized clients from connecting to a VLAN unless these clients are authorized by the server.

Overview

802.1x Port Security:

- Prevents unauthorized clients from connecting to a VLAN
- Can be configured on a per-port basis

Example

The following is an examples of how the 802.1x Port Security feature is used.

Example 1#: Enable 802.1x Authentication on One Port in a VLAN

The following example shows how to enable 802.1x authentication on one port, and to allow only the user with the name “adam” to access the VLAN.

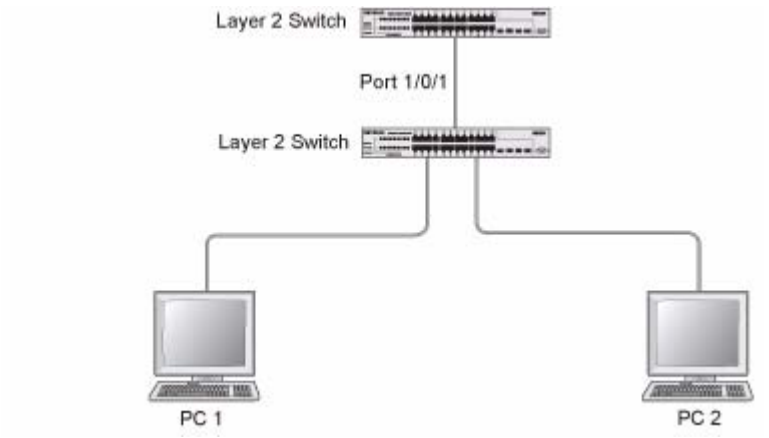


Figure 26-1

The example is shown as CLI commands and as a Web interface procedure.

CLI Commands

To use the CLI to enable 802.1x authentication on one port, and to allow only the user with the name “adam” to access the VLAN, enter the following CLI commands:

```
Create a VLAN 100, then add 1/0/1 to this VLAN and assign IP address
192.168.100.1 to it.
(Netgear Switch)#vlan database
(Netgear Switch) (Vlan)#vlan 100
(Netgear Switch) (Vlan)#vlan routing 100
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#vlan participation include 100
(Netgear Switch) (Interface 1/0/1)#vlan pvid 100
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface vlan 100
(Netgear Switch) (Interface-vlan 100)#routing
(Netgear Switch) (Interface-vlan 100)#ip address 192.168.100.1 255.255.255.0
(Netgear Switch) (Interface-vlan 100)#exit

Enable ip routing on the switch.
(Netgear Switch) (Config)#ip routing

Add a new user named adam.
(Netgear Switch) (Config))#users name adam
```

```
Add a new listname named dot1xList.
(Netgear Switch) (Config)#authentication login dot1xList

Enable 802.1x on the switch.
(Netgear Switch) (Config)#dot1x system-auth-control

Permit the user adam to login.
(Netgear Switch) (Config)#dot1x login adam dot1xList

Permit 4 users to login simultaneously.
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#dot1x max-user 4

Enable the MAC-based method. This method permits multi-user login through one
port.
(Netgear Switch) (Interface 1/0/1)#dot1x port-method macbased
(Netgear Switch) (Interface 1/0/1)#exit
```

Web Interface Procedure

To use the Web Interface to enable 802.1x authentication on one port, and to allow only the user with the name “adam” to access the VLAN, proceed as follows:

1. Create VLAN 100 with IP address 192.168.100.1:

a. From the main menu, select Routing > VLAN > VLAN Routing Wizard. A screen similar to the following displays.

Figure 26-2

b. Enter the following information in the VLAN Routing Wizard:

- In the Vlan ID field, enter **100**.
- In the IP Address field, enter **192.168.100.1**.
- In the Network Mask field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display:

d. Click the gray box under port 1 twice until **U** displays. The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 100.

2. Enable IP Routing:

a. From the main menu, select Routing > IP > Basic > IP Configuration. A screen similar to the following displays.

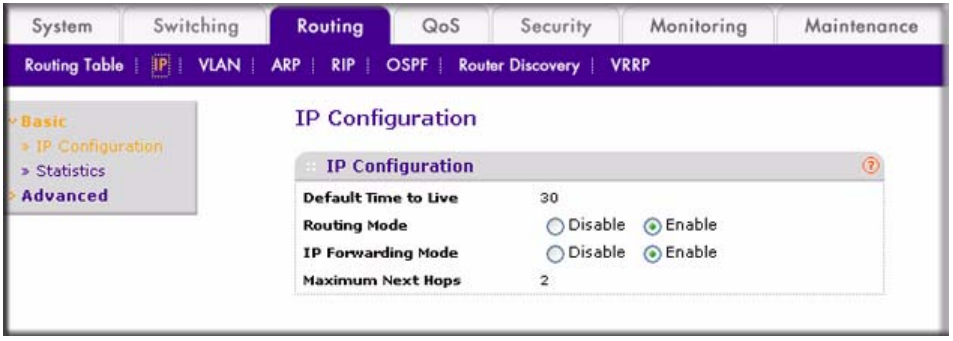


Figure 0-1

b. Under IP Configuration, make the following selections:

- Next to Routing Mode, select the **Enable** radio button.
- Next to IP Forwarding Mode, select the **Enable** radio button.

c. Click **Apply** to enable IP Routing.

3. Add a new user account with the name “adam”:

   a. From the main menu, select Security > Management Security > User Configuration > User Management. A screen similar to the following displays.

Figure 26-3

   b. Under Manage Users, in the User Name field, enter “adam” (without the quotes).

   c. Click **Add**.

4. Add a new authentication list with the name “dot1xList”:

   a. From the main menu, select Security > Management Security > Login > Authentication. A screen similar to the following displays.

Figure 26-4

   b. Under Authentication List, in the List Name field, enter “dot1xList” (without the quotes).

   c. Click **Add**.

5. Enable port authentication:

   a. From the main menu, select Security > Port Authentication > Basic > 802.1x Configuration. A screen similar to the following displays.

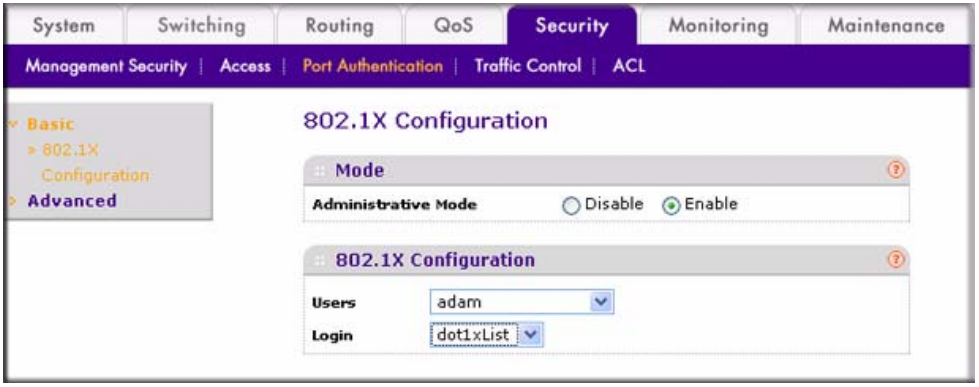


Figure 26-5

   b. Under Mode, next to Administrative Mode, select the **Enable** radio button.

   c. Under 802.1X Configuration, select the following:

      - Select **adam** from the Users pulldown menu.
      - Select **dot1xList** from the Login pulldown menu.

   d. Click **Apply** to save the changes.

6. Configure the MAC-based port method:

   a. From the main menu, select Security > Port Authentication > Advanced > Port Authentication. A screen similar to the following displays.

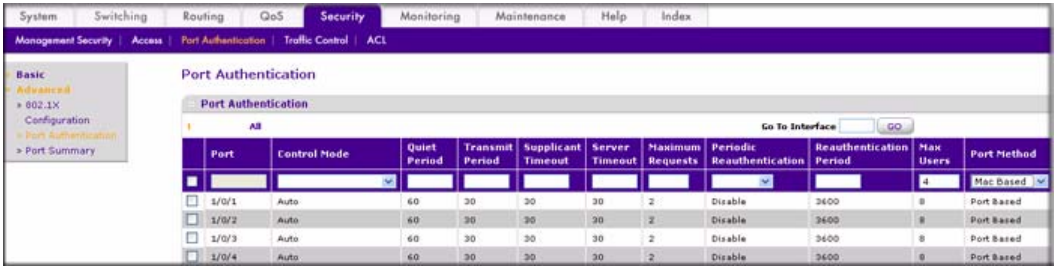


Figure 26-6

b. Under Port Authentication, enter the following information:

- In the Max Users field, enter **4**.
- Select **Mac based** from the Port Method pulldown menu.

c. Click **Apply** to save the settings.

Chapter 27
Double VLANs

This section describes how to configure the Double VLAN (DVLAN) feature on the switch. A DVLAN is a way to pass traffic of customers who have multiple VLANs from one customer domain to another customer domain. Custom VLAN IDs are preserved and a provider service VLAN ID is added to the traffic so that the traffic can pass the metro core in a simple and cost-effective manner.

Overview

Double VLANs:

- Pass customer traffic from one customer domain to another through the metro core
- Select customer ports and a service provider port

Example

Example 1#: Enable a Double VLAN on a VLAN

In the following example, the two switches have the same configuration.

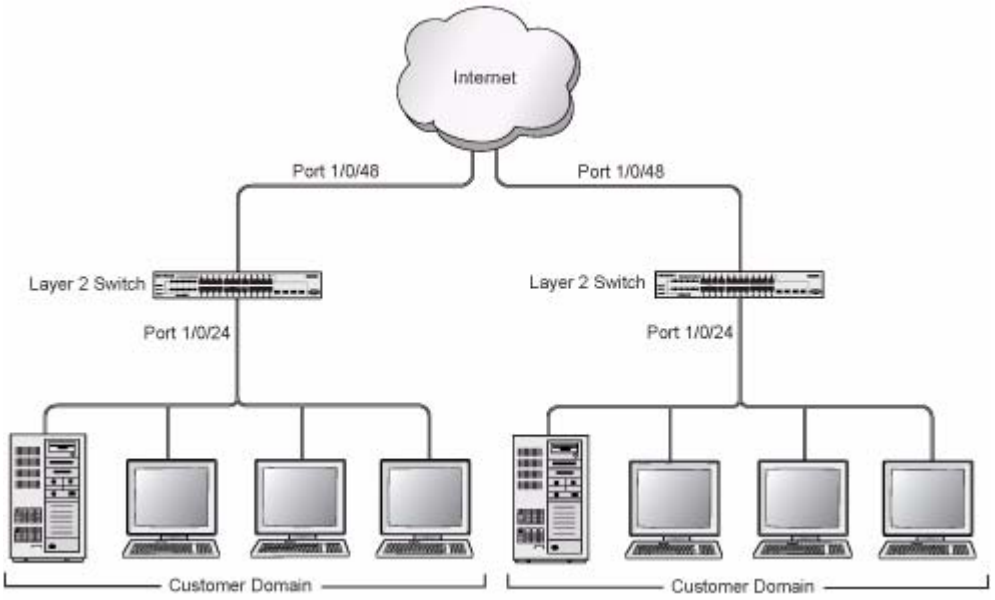


Figure 27-1

The example is shown as CLI commands and as a Web interface procedure.

CLI Commands

To use the CLI to enable a double VLAN on a VLAN, enter the following CLI commands:

```
Create a VLAN 200.
(Netgear Switch)#vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#exit

Add interface 1/0/24 to VLAN 200, add pvid 200 to the port.
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 200
(Netgear Switch) (Interface 1/0/24)#vlan participation include 200
(Netgear Switch) (Interface 1/0/24)#exit

Add interface 1/0/48 to the VLAN 200 in a tagging mode.
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan participation include 200
(Netgear Switch) (Interface 1/0/48)#vlan tagging 200
(Netgear Switch) (Interface 1/0/48)#exit
```

```
Select interface 1/0/48 as the provider port.
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#mode dvlan-tunnel
(Netgear Switch) (Interface 1/0/48)#exit
```

Web Interface Procedure

To use the Web Interface to enable a double VLAN on a VLAN, proceed as follows:

1. Create static VLAN 200:

a. From the main menu, select Switching > VLAN > Basic > VLAN Configuration. A screen similar to the following displays.

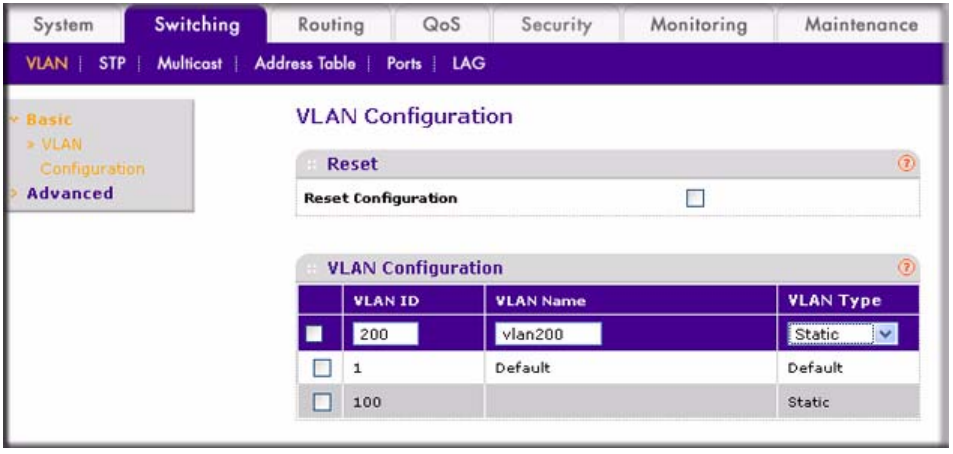


Figure 27-2

b. Under VLAN Configuration, enter the following information and make the following selection:

- In the VLAN ID field, enter **200**.
- In the VLAN Name field, enter **vlan200**.
- Select **Static** from the VLAN Type pulldown menu.

c. Click **Add**.

2. Add ports 24 and 48 to VLAN 200.

a. From the main menu, select Switching > VLAN > Advanced > VLAN Membership. A screen similar to the following displays.

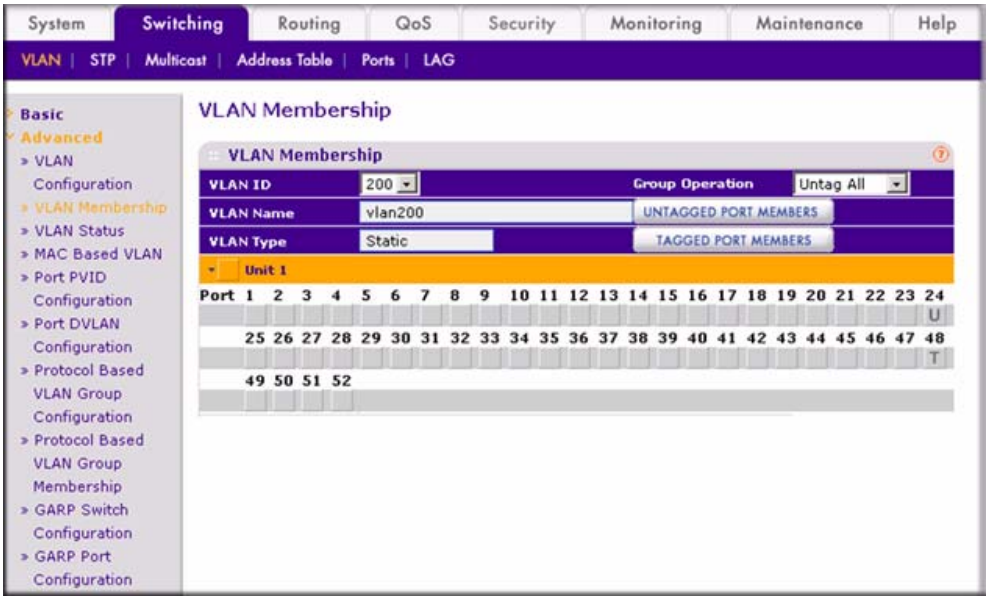


Figure 27-3

b. Under VLAN Membership, select **200** from the VLAN ID pulldown menu.

c. Click **Unit 1**. The ports display:

- Click the gray box under port 24 twice until **U** displays. The U specifies that the egress packet is untagged for the port.
- Click the gray box under port 48 once until **T** displays. The T specifies that the egress packet is tagged for the port.

d. Click **Apply** to save the settings.

3. Change the Port VLAN ID (PVID) of port 24 to 200:

a. From the main menu, select Switching > VLAN > Advanced > Port PVID Configuration. A screen similar to the following displays.

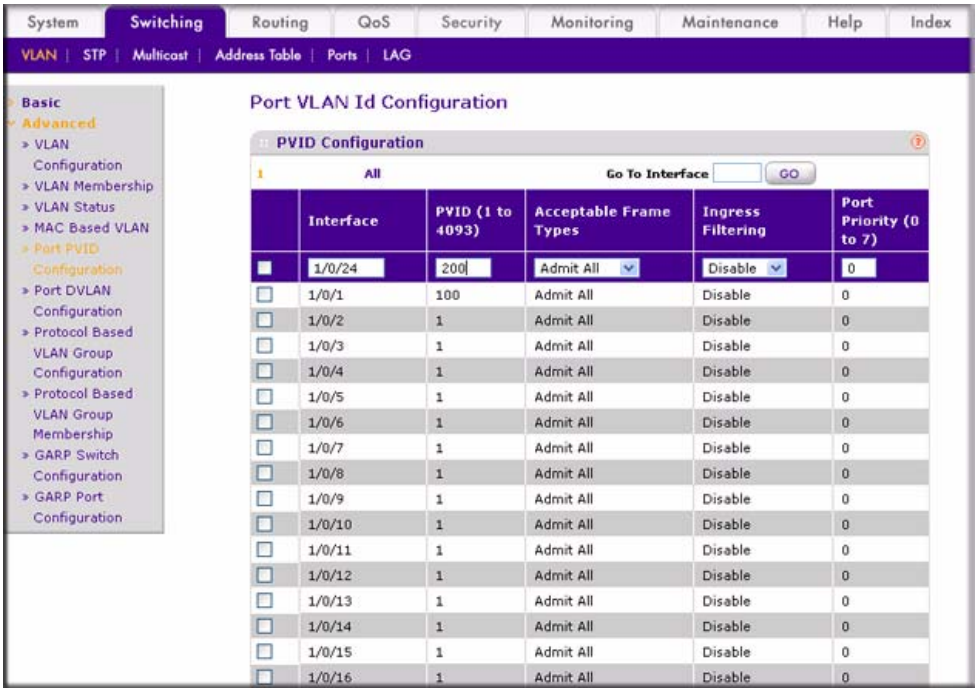


Figure 27-4

b. Under PVID Configuration, scroll down to interface 1/0/24 and select the chechbox for that interface. 1/0/24 now appears in the Interface field at the top.

c. Under PVID Configuration, in the PVID (1 to 4093) field, enter **200**.

d. Click **Apply** to save the settings.

4. Configure port 48 as the provider service port:

a. From the main menu, select Switching > VLAN > Advanced > Port DVLAN Configuration. A screen similar to the following displays.

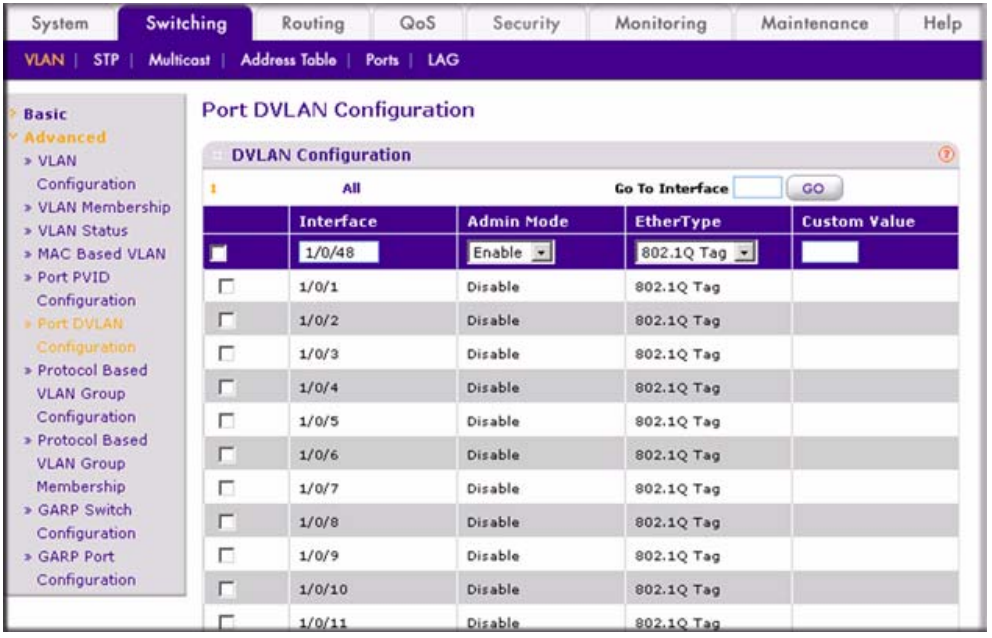


Figure 27-5

b. Under DVLAN Configuration, scroll down to interface 1/0/48 and select the chechbox for that interface. 1/0/48 now appears in the Interface field at the top.

c. Select **Enable** from the Admin Mode pulldown menu.

d. Click **Apply** to save the settings.

Index

Numerics

802.1x port security *26-1*

A

ACL *9-1*
add *4-5*
apply *4-5*
ARP *7-21*

C

cancel *4-5*
command
  archive *20-16*
  archive download-sw *20-8*
  clear config *2-14*
  clock timezone *18-4*
  copy nvram errorlog *2-13*
  copy nvram startup-config *2-12*, *2-13*
  copy nvram traplog *2-13*
  copy system image *2-13*
  copy system running-config nvram startup-config *2-12*, *2-14*
  cos-queue min-bandwidth *10-5*
  ezconfig *3-1*
  ip igmpsnooping *22-2*
  ip proxy-arp *7-22*
  logout *2-12*
  mac access list *9-38*
  mac access-group *9-40*
  member *20-15*
  monitor session 1 mode *17-3*
  monitor session 1 source interface *17-4*
  movemanagement *20-14*
  network parms *2-12*
  no clibanner *21-2*
  permit *9-41*
  permit any *9-39*
  port security *13-3*, *17-4*
  reload *2-14*
  script *15-2*
  script apply running-config.scr *15-2*
  script delete *15-2*
  script list *15-2*
  session-limit *16-3*
  session-timeout *16-3*
  set classofservice trust mode *10-4*
  show classofservice ip-precedence mapping *10-5*
  show classofservice trust *10-4*
  show hardware *2-11*
  show igmpsnooping *12-2*
  show ip interface *7-22*
  show ip vlan *7-5*
  show logging *19-3*
  show logging buffered *19-3*
  show logging hosts *19-4*
  show logging traplogs *19-4*
  show loginsession *2-11*
  show mac access-lists *9-42*
  show mac-address-table igmpsnooping *12-2*
  show monitor session *17-2*
  show network *2-5*, *2-12*, *16-2*
  show port *20-11*
  show port all *17-2*, *20-15*
  show port interface *17-2*
  show port security *13-3*
  show port security on a specific interface *13-3*
  show port-channel all *6-2*
  show sntp *18-1*
  show sntp client *18-2*
  show sntp server *18-2*
  show supported switchtype *20-15*
  show switch *20-8*
  show telnet *16-2*
  show users *2-11*
  sntp client mode unicast *18-3*
  sntp server *18-3*

switch priority 20-6
switch renumber 20-14
traceroute 14-1
traffic-shape 10-7
transport output telnet 16-3
users passwd 2-11

configuration scripting 15-1

CoS 10-1
drop precedence configuration 10-3
per-interface basis 10-3
port egress queue configuration 10-2
queue mapping 10-1
traffic shaping 10-6
untrusted ports 10-2

D

delete 4-5

DHCP server
dynamic mode 24-1
manual mode 24-4

DiffServ
edge device 11-1
interior node 11-1
VoIP support 11-4

DNS 23-1

DSCP 10-2

DVLAN 27-1

E

Easy Setup Wizard 2-9

Ezconfig utility 3-1

G

gaming 22-1

I

IGMP
IGMP snooping 12-1
IGMPv3 12-1

IGMP querier 22-1

IGMP snooping 22-1

in-band connectivity
BootP 2-5
DHCP 2-5
EIA-232 2-5, 2-6

initial configuration procedure 2-9

interpreting log files 19-2

IP routing
ARP 7-21
OSPF 7-15
port routing 7-1, 7-2
RIP 7-12
VLAN routing 7-4
VLAN routing OSPF configuration 7-10
VLAN routing RIP configuration 7-5, 7-7

IPTV 22-1

L

link aggregation (LAG) 6-1

M

MAC ACL 9-1

N

NVT 16-1

O

OSPF 7-1, 7-2, 7-10, 7-15

outbound Telnet 16-1

out-of-band connectivity 2-7

P

password
change the admin password 3-2

permit 9-41

port mirroring 17-1

port security 13-1

pre-login banner 21-1

private edge VLAN 5-1

protected ports *25-1*

Q

QoS
- class *11-1*
- policy *11-1*
- service *11-2*

R

refresh *4-5*

RIP *7-1*, *7-2*, *7-7*, *7-12*

S

SNMP V3 user profile *4-6*

SNTP *18-1*

static host name *23-1*

switch
- FSM family of switches *20-1*
- GSM family of switches *20-1*
- IP address *3-2*
- name *3-3*
- saving the configuration *3-3*

switch stack
- cabling *20-4*
- configuration files *20-8*
- configuration scenarios *20-9*
- management connectivity *20-9*
- master (re-)election *20-5*
- member numbers *20-5*
- member priority values *20-6*
- membership *20-3*
- offline configuration *20-6*
- software compatibility *20-8*
- stacking recommendations *20-11*

syslog *19-1*

T

traceroute *14-1*

traffic shaping *10-6*

U

untrusted ports *10-2*

V

video streaming *22-1*

VLAN *5-1*

VRRP *8-1*

W

web interface
- index page *4-5*
- main tags *4-4*
- saving the configuration *4-5*
- sub tags *4-5*
- web control buttons *4-5*

WRED *10-1*